

Christopher Marcus, P.C.
John T. Weber
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

James H.M. Sprayregen, P.C.
Michael B. Slade (*pro hac vice* pending)
Alexandra Schwarzman (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
300 North LaSalle Street
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200

Proposed Counsel to the Debtors and Debtors in Possession

**UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK**

In re:))
)	Chapter 11
))
21st CENTURY ONCOLOGY HOLDINGS, INC., <i>et al.</i> , ¹)	Case No. 17-22770 (RDD)
))
Debtors.)	(Jointly Administered)
))
21st CENTURY ONCOLOGY HOLDINGS, INC., <i>et al.</i> ,))
))
Plaintiff,)	Adversary Proceeding No.
))
v.)	_____
))
STEVEN BREHIO; ROBERT RUSSELL; JAMES))
CORBEL; ROXANNE HAATVEDT; VENETA))
DELUCCHI; CARL SCHMITT; MATTHEW BENZION;))
KATHLEEN LaBARGE; STACEY SCHWARTZ;))
TIMOTHY MEULENBERG; STEPHEN WILBUR;))
JACKIE GRIFFITH; JUDITH CABRERA; AND))
SHARON MacDERMID))
))
Defendants.))
))

¹ Each of the Debtors in the above-captioned jointly administered chapter 11 cases and their respective tax identification numbers are set forth in the *Order Directing Joint Administration of Chapter 11 Cases* [Docket No. 30]. The location of 21st Century Oncology Holdings, Inc.'s corporate headquarters and the Debtors' service address is: 2270 Colonial Boulevard, Fort Myers, Florida 33907.

**VERIFIED ADVERSARY COMPLAINT TO EXTEND AUTOMATIC STAY OR, IN
THE ALTERNATIVE, FOR PERMANENT INJUNCTIVE RELIEF
INTRODUCTION AND NATURE OF THE CASE**

NATURE OF THE ACTION

1. Before the debtors and debtors in possession (collectively the “*Debtors*”) commenced these chapter 11 cases, a series of lawsuits were filed against certain Debtors and their affiliates, alleging that as the result of a third party cyberattack on Debtor 21st Century Oncology Services, Inc., personal information was made public (the “*Data Breach Lawsuits*”). The Data Breach Lawsuits consisted of putative nationwide and/or statewide class actions, all of which were consolidated by the Judicial Panel on Multidistrict Litigation before a United States District Judge located in Tampa, Florida. *See In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 214 F. Supp. 3d 1357, 1358 (JPML 2016). Following consolidation, the plaintiffs filed a consolidated class action complaint, and the defendants filed a motion to dismiss, which was pending when these chapter 11 cases.

2. The defendants in the Data Breach Lawsuits are Debtor 21st Century Oncology Investments, LLC, and one non-debtor, 21st Century Oncology of California, A Medical Corporation (“*21C California*”). While the Data Breach Lawsuits against Debtor 21st Century Oncology Investments, LLC are clearly stayed on the petition date by 11 U.S.C. § 362, plaintiffs in the consolidated class action complaint have not agreed to stay the entire matter pending confirmation of a plan of reorganization.

3. The Debtors thus file this motion asking the Court to extend the automatic stay to cover non-debtor 21C California, who is named as a defendant in the Data Breach Lawsuits but is not a Debtor (although it has indemnity rights against the Debtors in any event). In the alternative, the Debtors ask this Court to enter a preliminary injunction barring the pursuit of the Data Breach Lawsuits until the confirmation of a plan of reorganization in these cases.

JURISDICTION AND VENUE

4. This Court has jurisdiction over the parties and the subject matter of this proceeding pursuant to 28 U.S.C. §§ 157 and 1334.

5. This adversary proceeding is a core proceeding within the meaning of 28 U.S.C. § 157(b)(2)(A), (E) and (G).

6. Venue of this adversary proceeding is proper pursuant to 28 U.S.C. § 1409.

7. The statutory bases for the relief requested in this Complaint are sections 362 and 105 of title 11 of the United States Code, 11 U.S.C. §§ 101-1532 (the “*Bankruptcy Code*”) and Rule 7001 of the Federal Rules of Bankruptcy Procedure.

THE PARTIES

8. The Debtors comprise a leading, global, physician-led provider of integrated cancer care services, providing comprehensive care to patients across the United States, South America, and Latin America. Debtor 21st Century Oncology Investments, LLC, is a Delaware limited liability company with its primary place of business in Florida, and it is the direct or indirect owner of the other Debtors.

9. On information and belief, Defendant Steven Brehio is an individual domiciled in Rhode Island.

10. On information and belief, Defendant Robert Russell is an individual domiciled in Arizona.

11. On information and belief, Defendant James Corbel is an individual domiciled in California.

12. On information and belief, Defendant Roxanne Haatvedt is an individual domiciled in California.

13. On information and belief, Defendant Veneta Delucci is an individual domiciled in California.

14. On information and belief, Defendant Carl Schmitt is an individual domiciled in Florida.

15. On information and belief, Defendant Matthew Benzion is an individual domiciled in Florida.

16. On information and belief, Defendant Kathleen LaBarge is an individual domiciled in Florida.

17. On information and belief, Defendant Stacey Schwartz is an individual domiciled in Florida.

18. On information and belief, Defendant Timothy Meulenberg is an individual domiciled in Florida.

19. On information and belief, Defendant Stephen Wilbur is an individual domiciled in Florida.

20. On information and belief, Defendant Jackie Griffith is an individual domiciled in Kentucky.

21. On information and belief, Defendant Judith Cabrera is an individual domiciled in Massachusetts.

22. On information and belief, Defendant Sharon MacDermid is an individual domiciled in New Jersey.

23. Together, Brehio, Russell, Corbel, Haatvedt, Delucchi, Schmitt, Benzion, LaBarge, Schwartz, Meulenberg, Wilbur, Griffith, Cabrera, and MacDermid are referred to hereinafter as the "***Data Breach Plaintiffs***."

FACTUAL BACKGROUND

24. Due to the varied state regulatory landscape for health care services, the Debtors are unable to employ physicians and other medical professionals directly in certain states in which they operate. As a result, the Debtors have developed two distinct business models. First, the Debtors own treatment facilities and directly employ the medical professionals working therein. In the second model (the “*MSA Model*”), the Debtors contract with private physician groups and provide a variety of administrative, financial, and management services to such physician groups pursuant to exclusive, long-term services agreements.

25. California is one of the states that prohibits the corporate practice of medicine and requires that medical services be provided at physician-owned clinics. As such, in California the Debtors utilize the MSA Model, contracting with physician-owned facilities to provide certain administrative and financial services, including non-physician clinical and administrative staff, operations management, purchasing assistance, managed care contract negotiation assistance, reimbursement, billing, and collections assistance, information technology, human resource and payroll services, and compliance, accounting, and treasury functions.

26. 21C California is a professional corporation organized under California law that provides cancer treatment services at several locations in California. The Debtors have partnered with 21C California under the MSA Model. Specifically, Debtor California Radiation Therapy Management Services, Inc. and 21C California are party to a Management Services Agreement, dated May 1, 2016 (as amended, modified and supplemented from time to time, the “*21CC MSA*”), attached hereto as Exhibit A.

27. Pursuant to the 21CC MSA, the Debtors are required to provide 21C California with, among other things: (a) all support personnel including, but not limited to, technicians, physicists, dosimetrists, nurses, receptionists, secretaries, clerks and other personnel; (b) all

furniture and medical equipment and maintenance of such equipment; (c) all medical supplies as are necessary for patient care and treatment; (d) recordkeeping services in accordance with applicable law concerning confidentiality and retention; (e) billing and collection services; (f) business officer services; and (g) services related to the scheduling of patient appointments.

In consideration for these services, the Debtors receive a management fee.

28. The 21CC MSA contains the following indemnification obligations if favor of the 21C California (the “***MSA Indemnity Obligations***”):

[The Debtors] shall indemnify, hold harmless and defend [21C California], its officers, directors, shareholders, employees, agents and independent contractors . . . from and against any and all liabilities, losses, damages, claims, causes of action, and expenses (including reasonable attorneys’ fees and disbursements) . . . caused or asserted to have been caused, directly or indirectly, by or as a result of the performance of medical services or any other acts or omissions by [the Debtors] and/or its partners, agents, employees and/or subcontractors

(21CC MSA, § 16(k)). Accordingly, Debtor California Radiation Therapy Management Services, Inc. is likely obligated to indemnify 21C California with respect to any legal costs and any damages arising in connection with the Data Breach Lawsuits.

29. The Data Breach Plaintiffs initiated the Data Breach Lawsuits through the filing of 18 separate complaints in various courts across the country. The lawsuits were consolidated by the Judicial Panel on Multidistrict litigation in the United States District Court for the Middle District of Florida (the “***Florida District Court***”), and a consolidated class action complaint was filed. *See Consolidated Class Action Complaint, In re 21st Century Oncology Customer Data Security Breach Litigation*, No. 8:16-md-2737 (MSS-AEP) (M.D. Fla. Jan. 1, 2017) [Docket No. 100] (the “***Data Breach Complaint***,” attached hereto as **Exhibit B** and, together with the Data Breach Lawsuits, the “***Data Breach Litigation***”).

30. Debtor 21st Century Oncology Investments, LLC, and non-debtor 21C California, are the two named defendants in the Data Breach Complaint. The Data Breach Complaint includes twenty-two separate causes of action.

31. The Data Breach Complaint alleges that in October 2015, Debtor 21st Century Oncology Services, Inc. was the victim of a cyberattack. (Ex. B., Data Breach Compl. ¶ 5.) To date, the perpetrators remain unidentified, but on November 13, 2015, the FBI notified the Debtors that a third party illegally obtained patient information and may have accessed the Debtors' database. (*Id.* ¶¶ 5, 96.) According to the Data Breach Complaint, in March 2016, Debtor 21st Century Oncology Holdings, Inc., sent notification letters to those whose information may have been affected by the cyberattack. (*Id.* ¶ 117.) The letter informed recipients that the FBI discovered that an unauthorized third-party may have accessed a database of the Debtors, and that the Debtors immediately hired a leading forensics team to support its investigation into the cyberattack, assess its systems, and bolster security. (*Id.*)

32. On February 21, 2017, Debtor 21st Century Oncology Investments, LLC, and co-defendant 21C California moved to dismiss the Data Breach Complaint. *See Motion to Dismiss, In re 21st Century Oncology Customer Data Breach Litigation*, No. 8:16-md-2737 (MSS-AEP) (M.D. Fla. Feb. 21, 2017) [Docket No. 116], attached hereto as **Exhibit C**. The motion argues that the Data Breach Complaint should be dismissed because, among other things, at least seven of the Data Breach Plaintiffs lack standing, and all of the allegations fail to state a claim upon which relief can be granted. The Florida District Court has not yet decided the motion.

33. On June 1, 2017, after being notified of the commencement of the Chapter 11 Cases chapter 11 cases, the Florida District Court ordered the entire case stayed, and requested

that 21C California submit a status report as to whether and in what form the Data Breach Litigation should proceed against 21C California in light of its status as a non-Debtor.

34. In response to the Florida District Court's direction, 21C California filed status reports stating that it believed the matter should continue to be stayed in its entirety, and that the Debtors would be seeking the relief requested herein. The Florida District Court has taken no further action.

35. There is no question that the Data Breach Plaintiffs will be well represented and will have the right to be heard in the Chapter 11 Cases. Separate and apart from their individual representation in the Data Breach Lawsuits and their representation by putative class counsel in the MDL, on June 8, 2017, the Office of the United States Trustee for the Southern District of New York appointed an official committee of unsecured creditors (the "***Creditors' Committee***") [Docket Nos. 92 & 94]. One of the plaintiffs in the Data Breach Complaint was appointed to the Creditors' Committee.

NATURE OF RELIEF REQUESTED

36. The Debtors seek a declaration that prosecution of the Data Breach Litigation against 21C California is stayed during the Chapter 11 Cases, pursuant to 11 U.S.C. §§ 362(a)(1) and (a)(3). In the alternative, the Debtors seek to enjoin prosecution of the Data Breach Complaint during the pendency of these Chapter 11 proceedings, pursuant to 11 U.S.C. § 105.

COUNT I

(Automatic Stay Declaratory Judgment)

37. The Debtors repeat and re-allege paragraphs 1-35 as if fully set forth herein.

38. Extension of the stay to cover all defendants in the Data Breach Litigation is warranted given the identity of interest between the Debtors and and the non-debtor affiliate defendant, 21C California.

39. As a threshold matter, Debtor 21st Century Oncology Investments, LLC, is the real party in interest in the Data Breach Lawsuits. The Debtor entities own and maintain the systems that are at issue in the Data Breach Litigation. The Debtors received the information from the FBI regarding the alleged data breach, and the Debtors are the entities that advised the public (including the Data Breach Plaintiffs) of the issue. The Data Breach Complaint does not identify any conduct specific to 21C California.

40. Regardless, the Debtors consider the claims against 21C California to be claims against the Debtors for several reasons.

41. First, due to the MSA Indemnity Obligations, the Debtors would likely be financially liable for judgments that may arise out of the Data Breach Litigation.

42. Second, at this time, the Debtors have every intention of maintaining their relationships with 21C California, which likely entails assuming the 21C MSA as part of the Chapter 11 plan process pursuant to section 365 of the Bankruptcy Code.

43. Accordingly, if the Data Breach Litigation is not stayed, the Debtors' cure costs under section 365 of the Bankruptcy Code, administrative priority expenses, will assuredly increase, and if there is an adverse judgment in the litigation, the Debtors will likely be responsible for payment in full under the assumed MSA Indemnity Obligations

44. If the Data Breach Lawsuits proceed, Debtors risk irreparable harm, including:

45. Impairment of Debtors' Assets: Any adverse judgment against 21C California in the Data Breach Litigation may give rise to indemnity claims against Debtors. Indeed, the mere

continuation of the action will require Debtors to deplete an insurance policy that is an asset of the estate and is currently funding the defense of the Data Breach Litigation. Absent a stay, the Data Breach Litigation will deplete the Debtors' assets by a significant amount of money during the course of the Chapter 11 Cases, regardless of the outcome.²

46. Collateral Estoppel or Issue Preclusion: If the Data Breach Litigation proceeds against non-debtor 21C California, there is a risk that the Debtors will be barred from challenging the judgment or re-litigating adverse factual or legal findings. This could result in adverse judgments or increased indemnification claims against Debtors at some point in the future.

47. In short, the continuation of the Data Breach Litigation would undermine and distract from the Debtors' chances for a successful Chapter 11 reorganization. Accordingly, this Court should extend the stay to cover all defendants in the Data Breach Litigation.

COUNT II

(Section 105 Injunction)

48. Debtors repeat and re-allege paragraphs 1-35 above as if fully set forth herein.

49. Alternatively, in the event the Court declines to extend the automatic stay, the Debtors seek an injunction pursuant to 11 U.S.C. § 105 barring the continued prosecution of the Data Breach Litigation pending confirmation of a plan of reorganization.

50. Section 105(a) of the Bankruptcy Code authorizes the court to issue "any order, process or judgment that is necessary or appropriate to carry out the provisions of this title."

² The Debtors' primary insurance carrier has agreed at the present time to cover defense costs for the Data Breach Litigation through a self-depleting insurance policy that has \$5 million of coverage. That policy is an asset of the estate and, absent a stay, will be depleted materially (if not exhausted entirely). The excess carrier has denied any obligation to provide coverage and has initiated a declaratory judgment lawsuit in Florida seeking a declaration that it has no obligations (to Debtors or non-Debtors). *See The Charter Oak Fire Ins. Co. v. 21st Century Oncology Investments, LLC, et al.*, No. 8:17-cv-582-MSS-AEP (M.D. Fla. filed Sept. 26, 2016).

11 U.S.C. § 105(a). Relief under § 105 is particularly appropriate where it would help the debtor confirm a plan of reorganization and/or preserve property of the debtor's estate. Here, as discussed above, the continuation of the Data Breach Litigation will diminish the property of the Debtors' estate and threaten their ability to confirm a plan of reorganization.

51. Pursuant to the broad powers of Section 105(a) and the applicable case law, a bankruptcy court may enjoin actions against non-debtors under various circumstances, including situations where non-debtor claims may affect property of the debtor's estate.

52. If the prosecution of the Data Breach Litigation is not enjoined, the Debtors will suffer irreparable harm, including the use of a self-depleting insurance policy that is an asset of the estate to cover legal fees, the distraction of personnel from the restructuring process and the possibility of being bound by adverse rulings against the defendants.

53. The likelihood of irreparable harm to the Debtors from the continuation of the Complaint far outweighs any risk of harm to the Data Breach Plaintiffs should the action be enjoined pending the Chapter 11 proceeding.

54. The injunctive relief sought by Debtors in this action will serve the public interest by promoting their speedy and successful reorganization—a benefit not only to Debtors themselves but to their employees, patients, vendors, and others who do business with Debtors on a daily basis. The injunctive relief sought herein will also serve the purpose of the automatic stay, which is to provide the Chapter 11 debtor with a period of breathing room in which to reorganize, so as to preserve its assets for the benefit all constituencies.

55. Based on the foregoing, the Debtors seek an injunction under 11 U.S.C. § 105 preventing defendants from prosecuting the Data Breach Complaint pending the confirmation of a plan of reorganization in the current Chapter 11 proceeding.

WHEREFORE, the Debtors respectfully request relief as follows:

- a) a declaratory judgment that the continued prosecution of the Data Breach Litigation is stayed pursuant to 11 U.S.C. § 362; or
- b) in the alternative, an injunction pursuant to 11 U.S.C. § 105 and 28 U.S.C. § 1651 preventing defendants from prosecuting the Complaint pending the confirmation of a plan of reorganization; and
- c) such other relief as the Court may find just and proper.

New York, New York
Dated: June 30, 2017

/s/ Christopher Marcus, P.C.

Christopher Marcus, P.C.

John T. Weber

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

- and -

James H.M. Sprayregen, P.C.

Michael B. Slade (*pro hac vice* pending)

Alexandra Schwarzman (admitted *pro hac vice*)

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

*Proposed Counsel to the Debtors
and Debtors in Possession*

VERIFICATION

I hereby verify under penalty of perjury that the statements in the Verified Complaint are true and correct based on my personal knowledge, information supplied to me by others, and my review of relevant documents.

/s/ Paul Rundell

Paul Rundell
Interim Chief Executive Officer
21st Century Oncology Holdings, Inc. and
each of its Debtor affiliates

Exhibit A

21CC MSA

THIRD ADDENDUM TO MANAGEMENT SERVICES AGREEMENT

This Third Addendum (the "Addendum") is entered into as of August 1, 2007, by and between CALIFORNIA RADIATION THERAPY MANAGEMENT SERVICES, INC., a California corporation ("Manager") and 21ST CENTURY ONCOLOGY OF CALIFORNIA A MEDICAL CORPORATION, a California medical corporation ("Medical Group"). This Addendum amends Sections 1.(a) of the Management Services Agreement dated May 1, 2006, as set forth below.

From and after the date here of,

(i) Section 1.(a) shall be amended to read as follows:

"(a) Management. The Manager will be responsible for general management and administration operations of the Office locations, excluding the provision of medical services, set forth on Exhibit B hereto. The Manager shall not engage in the practice of medicine."

Accepted: CALIFORNIA RADIATION THERAPY
MANAGEMENT SERVICES, INC.

By: /s/ David N.T. Watson
David N.T. Watson
Vice President

Accepted: 21ST CENTURY ONCOLOGY OF
CALIFORNIA, A MEDICAL
CORPORATION

By: /s/ Daniel E. Dosoretz
Daniel E. Dosoretz, M.D.
Vice President

EXHIBIT B

THIRD ADDENDUM TO MANAGEMENT SERVICES AGREEMENT

Office Locations and Manager Compensation

Office Location	Manager Compensation as a % of Net Collected Dollars
Palm Desert 77840 Flora Road Palm Desert, CA 92211	77 %
Santa Monica 2428 Santa Monica Boulevard Suite 103 Santa Monica, CA 90404	77 %
Beverly Hills Radiation Oncology 150 N. Robertson Blvd. Suite 160 Beverly Hills, CA 90221	77%
Vidya S. Bobba, M.D., Inc. 963 Butte Street Redding, CA 96001	77%

SECOND ADDENDUM TO MANAGEMENT SERVICES AGREEMENT

This Second Addendum (the "Addendum") is entered into as of November 1, 2006, by and between CALIFORNIA RADIATION THERAPY MANAGEMENT SERVICES, INC., a California corporation ("Manager") and 21ST CENTURY ONCOLOGY OF CALIFORNIA A MEDICAL CORPORATION, a California medical corporation ("Medical Group"). This Addendum amends Sections 1.(a) of the Management Services Agreement dated May 1, 2006, as set forth below.

From and after the date here of,

(i) Section 1.(a) shall be amended to read as follows:

"(a) Management. The Manager will be responsible for general management and administration operations of the Office locations, excluding the provision of medical services, set forth on Exhibit B hereto. The Manager shall not engage in the practice of medicine."

Accepted: CALIFORNIA RADIATION THERAPY
MANAGEMENT SERVICES, INC.

By: /s/ David M. Koeninger
David M. Koeninger
Chief Financial Officer

Accepted: 21ST CENTURY ONCOLOGY OF
CALIFORNIA, A MEDICAL
CORPORATION

By: /s/ Daniel E. Dosoretz
Daniel E. Dosoretz, M.D.
Vice President

EXHIBIT B

ADDENDUM TO MANAGEMENT SERVICES AGREEMENT

Office Locations and Manager Compensation

Office Location	Manager Compensation as a % of Net Collected Dollars
Palm Desert 77840 Flora Road Palm Desert, CA 92211	77 %
Santa Monica 2428 Santa Monica Boulevard Suite 103 Santa Monica, CA 90404	77 %
Beverly Hills Radiation Oncology 150 N. Robertson Blvd. Suite 160 Beverly Hills, CA 90221	77%

ADDENDUM TO MANAGEMENT SERVICES AGREEMENT

This Addendum (the "Addendum") is entered into as of August 1, 2006, by and between CALIFORNIA RADIATION THERAPY MANAGEMENT SERVICES, INC., a California corporation ("Manager") and 21ST CENTURY ONCOLOGY OF CALIFORNIA A MEDICAL CORPORATION, a California medical corporation ("Medical Group"). This Addendum amends certain sections of the Management Services Agreement dated May 1, 2006, which was assumed by Manager in conjunction with Manager's acquisition of certain assets from LHA, Inc. also on May 1, 2006, as set forth below.

From and after the date here of,

(i) Section 1.(a) shall be amended to read as follows:

"(a) Management. The Manager will be responsible for general management and administration operations of the Office locations, excluding the provision of medical services, set forth on Exhibit B hereto. The Manager shall not engage in the practice of medicine."

(ii) Section 1.(g) shall be added to read as follows:

"(g) Patient-Related Matters.

- (a) Patient Relations, Scheduling, Etc. Manager shall assist Medical Group in maintaining positive patient relations by, among other things, in conjunction with and at the direction of Medical Group: scheduling patient appointments; responding to patient grievances and complaints in matters other than medical evaluation, diagnosis, and treatment; and establishing and maintaining in Medical Group's name and on its behalf patient transfer arrangements to expedite referrals where medically necessary, as determined and requested by the attending physician.
- (b) Recordkeeping. Manager shall assist Medical Group in maintaining patient medical records in accordance with applicable laws concerning their confidentiality and retention, and promptly making such records available to Medical Group's employed providers, contracting providers and other appropriate recipients. Notwithstanding the foregoing sentence, patient medical records shall be and shall remain the property of Medical Group, and the content thereof shall be solely the responsibility of Medical Group.

(c) Quality Assurance.

- a. In General. Manager shall assist Medical Group, in accordance with criteria established by Medical Group, in the development and implementation of appropriate quality assurance programs, including development of performance and utilization standards, sampling techniques for case review, and preparation of appropriately documented studies. Notwithstanding the foregoing, Manager shall not perform any duties that constitute the corporate practice of medicine in California and all other states in which an Office at which the Medical Group provides patient medical services is located.
- b. Periodic Independent Review. On behalf of Medical Group, Manager may periodically perform quality assurance and utilization reviews through nurses employed by it; provided however, that Manager shall not engage in activities which constitute the practice of medicine under applicable law. Alternatively, Manager may periodically arrange for an independent quality assurance and utilization review to be performed by persons who are unrelated to Medical Group or Manager, or to any Affiliate of Medical Group or Manager, which has expertise in such areas, and which has been approved in advance by Medical Group. Such review shall include a random sampling of medical records (consistent with laws regarding the confidentiality of medical records), an analysis of Medical Group's quality assurance utilization review procedures, and an analysis of the appropriateness of costs associated with operating Medical Group's medical practice at the practice."

(iii) Section 1. (h) shall be added to read as follows:

"(h) Offices. Manager shall provide, manage and maintain the real property comprising the Offices and reasonable improvements during the term of this Agreement. In consultation with Medical Group, Manager shall oversee all management, maintenance and other decisions pertaining to the Offices consistent with the terms of this Agreement. Manager shall maintain the Offices in good condition and repair, reasonable wear and tear excepted. Manager shall provide such additional and/or replacement facilities as Medical Group and Manager agree, from time to time. Manager shall provide Medical Group with all utilities (including water, gas and electricity), heat, air conditioning, telephone, janitorial services and disposal services (including the disposal of medical wastes) required in connection with the operation of the Offices."

(iv) The first sentence of Section 4.(a) shall be amended to read as follows:

“(a) The Manager shall be paid, and Manager shall accept as payment for the full performance of its duties hereunder, an amount equal to the respective percentage of Net Collected Dollars for each Office as contained in Exhibit B hereto.”

(v) Section 2. shall be amended to read as follows:

“2. Term. The initial term of this Agreement shall commence as of May 1, 2006 (the “Commencement Date”) and, shall, unless sooner terminated as herein, continue until April 30, 2031, and shall be automatically renewed for successive five (5) year periods thereafter (collectively, the “Term”), provided that neither Manager nor the Medical Group shall have given notice of termination of this Agreement at least one hundred twenty (120) days before the end of the initial term or any renewal term.”

(vi) Sections 13.(a) and (b) shall be amended to read as follows:

“13. Restrictive Covenants.

- (a) During the Term of this Agreement and for three (3) years following the termination of this Agreement, Medical Group agrees that it shall not, directly or indirectly:
 - (i) engage in the ownership, operation or management of any radiation oncology practice or otherwise engage in the provision of radiation oncology services (whether as a separate business or in conjunction with any other business (a “Competing Business”) within an eight (8) mile radius of the Office (the “Service Area”)); or
 - (ii) have any interest, whether as owner, stockholder, partner, member, director, officer, employee or consultant in any Competing Business in the Service Area.
- (b) During the Term of this Agreement and for three (3) years following the termination of this Agreement, Medical Group agrees that it shall not, directly or indirectly, (i) solicit, encourage or advise patients serviced during the Term of this Agreement to obtain or seek professional services from any professional who is not an employee, independent contractor or partner of Medical Group, or (ii) solicit, encourage or advise any employees of Manager to terminate employment with Manager for any reason whatsoever. Notwithstanding the foregoing, nothing in this Agreement is intended to prevent Medical Group from referring a patient in need of specialty services not otherwise provided by Medical Group, or

for other reasons in the best interests of the patient, to another duly licensed professional or facility.”

(vii) Section 16(k) shall be added to read as follows:

“(k) Indemnification. Medical Group shall indemnify, hold harmless and defend Manager, its officers, directors, shareholders, employees, agents and independent contractors (the “Manager Parties”) from and against any and all liabilities, losses, damages, claims, causes of action, and expenses (including reasonable attorneys’ fees and disbursements (a “Manager Loss”)), caused or asserted to have been caused, directly or indirectly, by or as a result of the performance of medical services or any other acts or omissions by Manager and/or its partners, agents, employees and/or subcontractors (other than Manager) during the Term hereof except with respect to any Manager Loss which is the result of any gross or willful misconduct by a member of Manager Parties. Manager shall indemnify, hold harmless and defend Medical Group, its officers, directors, shareholders, employees, agents and independent contractors (the “Medical Group Parties”) from and against any and all liabilities, losses, damages, claims, causes of action, and expenses (including reasonable attorneys’ fees and disbursements) (a “Medical Group Loss”), caused or asserted to have been caused, directly or indirectly, by or as a result of the performance of medical services or any other acts or omissions by Manager and/or its partners, agents, employees and/or subcontractors (other than Manager) during the Term hereof except with respect to any Medical Group Loss which is the result of any gross or willful misconduct by a member of Medical Group Parties.”

Accepted: CALIFORNIA RADIATION THERAPY
MANAGEMENT SERVICES, INC.

By: /s/ David M. Koeninger
David M. Koeninger
Chief Financial Officer

Accepted: 21ST CENTURY ONCOLOGY OF
CALIFORNIA, A MEDICAL
CORPORATION

By: /s/ Daniel E. Dosoretz
Daniel E. Dosoretz, M.D.
Vice President

EXHIBIT B

ADDENDUM TO MANAGEMENT SERVICES AGREEMENT

Office Locations and Manager Compensation

Office Location	Manager Compensation as a % of Net Collected Dollars
Palm Desert 77840 Flora Road Palm Desert, CA 92211	77 %
Santa Monica 2428 Santa Monica Boulevard Suite 103 Santa Monica, CA 90404	77 %

**ASSIGNMENT AND ASSUMPTION OF
MANAGEMENT SERVICES AGREEMENT**

THIS ASSIGNMENT AND ASSUMPTION AGREEMENT (this "Agreement") made this 1st day of May, 2006 between and among LHA, Inc., a California corporation ("Assignor"), California Radiation Therapy Management Services, Inc., a California corporation ("Assignee"); and 21st Century Oncology of California, a Medical Corporation ("21st Century").

RECITAL:

1. Assignor and 21st Century are parties to that certain Management Services Agreement, attached hereto as Exhibit A (the "Management Services Agreement").

2. Assignee and Assignor have entered into an Asset Purchase Agreement dated as of April 26, 2006, providing for the acquisition by Assignee of substantially all of the assets of Assignor (the "Transaction").

3. In connection with and only upon the consummation of the Transaction, Assignor desires to assign all of its right, title and interest in and to the Management Services Agreement to Assignee as of the date hereof.

4. Assignee desires to accept the assignment of the Management Services Agreement and to assume all rights and obligations of Assignor under the Management Services Agreement as of the date hereof.

5. Assignee and Assignor desire to secure the consent of 21st Century to the assignment and assumption of the Management Services Agreement.

6. Assignee agrees to accept such assignment in accordance with the terms, conditions, covenants and agreements hereinafter set forth.

NOW, THEREFORE, for and in consideration of the mutual covenants contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows.

1. Assignment. Assignor hereby assigns, transfers, grants, bargains, delivers, conveys and sets over (collectively, the "Assignment") to Assignee all of Assignor's legal, beneficial and other rights, title, benefit, privileges, and interest in and to the Management Services Agreement.

2. Assumption. Assignee hereby accepts the Assignment and hereby assumes, covenants and agrees to perform and observe all of the undertakings and obligations to be performed or observed by Assignor as a party to the Management Services Agreement.

3. Consent of 21st Century. 21st Century hereby consents to the Assignment.

4. Indemnification. Assignee hereby agrees to indemnify and hold harmless Assignor and its officers, directors, shareholders, employees, agents, representatives

and affiliates from and against all claims, suits, obligations, liabilities, damages and expenses, including, without limitation, reasonable attorneys' fees, based upon, arising out of or resulting from any obligation, contract or liability relating to the Management Services Agreement, but only to the extent such obligation, contract or liability accrues, or is otherwise attributable to the period on and after the date hereof.

5. Binding Effect. This instrument shall inure to the benefit of Assignee and Assignor and their successors and assigns and shall be binding upon the Assignor and Assignee and their respective successors and assigns.

6. Further Assurances. Assignor further covenants and agrees that, from time to time after the delivery of this instrument, at Assignee's request and without further consideration, Assignor will do, furnish, execute, acknowledge and deliver, or cause to be done, executed, acknowledged and delivered, all such further acts, conveyances, transfers, assignments, documents and assurances as reasonably may be requested by Assignee (or Assignee's counsel) more effectively to convey to, transfer to and vest in Assignee all rights, title and interest in and to the Management Services Agreement assigned hereunder provided such is without cost or liability to the Assignor.

7. Waivers and Amendments. This Agreement may be amended, modified, superseded, canceled, renewed or extended, and the terms and conditions hereof may be waived, only by a written instrument signed by the Assignor and Assignee or, in the case of a waiver, by the party waiving compliance. No delay on the part of any party in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any waiver on the part of any party of any right, power or privilege hereunder, nor any single or partial exercise of any right, power or privilege hereunder, preclude any other or further exercise thereof or the exercise of any other right, power or privilege hereunder. The rights and remedies herein provided are cumulative and are not exclusive of any rights or remedies which any party may otherwise have at law or in equity.

8. Governing Law. This Agreement shall be governed and construed in accordance with the laws of the State of California, without regard to its conflict of law principles.

9. Counterparts. This Agreement may be executed in two or more counterparts, each of which shall be deemed an original and all of which when taken together shall constitute a single instrument.

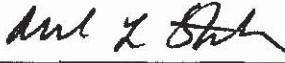
10. Release of Assignor by 21st Century. Effective with the execution and delivery of this Assignment, 21st Century hereby releases Assignor and its directors, officers, shareholders, employees, attorneys, accountants, agents and representative with respect to any and all claims, demands, liens, agreements, contracts, covenants, actions, suits, causes of action, obligations, controversies, debts, costs, expenses, damages, judgments, administrative or criminal complaints or proceedings, orders and liabilities of whatever kind and nature in law, equity or otherwise, whether now known or unknown, suspected or unsuspected, which have existed or may have existed, or which do exist, as of the date of this Assignment, including, but without in any respect limiting the generality of the foregoing, any and all claims which were, or might, or

could have been alleged, and any and all claims arising from or out of the acts, transactions, and occurrences relating to the execution and delivery of the Management Services Agreement.

[SIGNATURE PAGE TO FOLLOW]

IN WITNESS WHEREOF, the parties have executed this Agreement on the date first written above.

LHA, INC.

By: 

Name: Michael L. Steinberg, M.D.
Title: Chairman and Chief Financial Officer

By: 

Name: Leopold T. Avallone, M.D.
Title: President

CALIFORNIA RADIATION THERAPY
MANAGEMENT SERVICES, INC.

By: _____

Name:
Title:

21ST CENTURY ONCOLOGY of CALIFORNIA,
A MEDICAL CORPORATION

By: _____

Name:
Title:

IN WITNESS WHEREOF, the parties have executed this Agreement on the dated first written above.

LHA, INC.

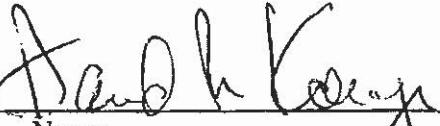
By: _____

Name: Michael L. Steinberg, M.D.
Title: Chairman and Chief Financial Officer

By: _____

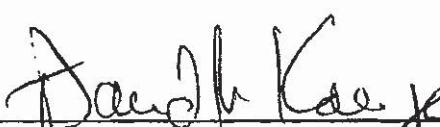
Name: Leopold T. Avallone, M.D.
Title: President

CALIFORNIA RADIATION THERAPY
MANAGEMENT SERVICES, INC.

By: 

Name: David M. Koeninger
Title: Executive Vice President - Chief Financial Officer
Radiation Therapy Services, Inc.

21ST CENTURY ONCOLOGY of CALIFORNIA,
A MEDICAL CORPORATION

By: 

Name: David M. Koeninger
Title: Executive Vice President - Chief Financial Officer
Radiation Therapy Services, Inc.

EXHIBIT A

Management Services Agreement

MANAGEMENT SERVICES AGREEMENT

MANAGEMENT SERVICES AGREEMENT (the "Agreement") made as of the 1st day of May, 2006; by and between LHA, Inc., a California corporation ("Manager") and 21st Century Oncology of California, a Medical Corporation ("Medical Group").

RECITALS:

1. Medical Group is a provider of radiation oncology services.
2. Medical Group wishes to engage the Manager as an independent contractor, to provide it with certain office facilities, equipment, supplies and administrative services at a practice located at 2428 Santa Monica Boulevard, Suite 103, Santa Monica, California (the "Office").

NOW, THEREFORE, for good and valuable consideration, the parties agree as follows:

1. **Manager's Undertakings.**

(a) **Management.** The Manager will be responsible for general management and administration operations of the Office, excluding the provision of medical services. The Manager shall not engage in the practice of medicine.

(b) **Personnel.** Manager shall provide, on behalf of Medical Group, all support personnel including, but not limited to, technicians, physicists, dosimetrists, nurses, receptionists, secretaries, clerks, management personnel and/or other personnel as necessary, as determined by the Manager in consultation with Medical Group ("Manager Personnel"). Manager shall be responsible for recruiting, managing, supervising compensating and terminating the Manager Personnel. Manager shall be responsible for all salaries, fringe benefits, taxes and insurance necessary with respect to such individuals. At such times as the Manager Personnel are providing services on Medical Group's behalf, Medical Group shall have authority and responsibility for (i) the supervision and control of the Manager Personnel (while providing services on behalf of the Medical Group) and (ii) determining the means and methods by which the Manager Personnel provides services hereunder.

(c) **Equipment.** Manager hereby leases to the Medical Group the furniture, fixtures and equipment at the Office described on Exhibit A hereof (the "Equipment") and Medical Group hereby leases such Equipment from Manager. Manager shall maintain all Equipment in good repair, condition and working order, and shall furnish all parts and services for the Equipment reasonably required therefor including, without limitation, preventive and routine maintenance as necessary and appropriate, as determined by Manager in its sole discretion. The parties agree and acknowledge that Medical Group shall be free to exercise its professional judgment with respect to the use of the Equipment. The Equipment provided hereunder shall, at all times, be and remain the property of Manager. Medical Group shall not cause or permit the Equipment to be subject to any lien, levy, attachment, encumbrance or charge, or to any judicial process of any kind whatsoever, and shall not remove the Equipment from the Office without the prior written consent of Manager.

(d) Licensing, Inspection and Regulatory Fees. Manager shall be responsible for all licensing, inspection and regulatory fees incurred in connection with the services provided by Manager hereunder.

(e) Supplies. Manager shall provide Medical Group with such office and medical supplies as are necessary for patient care and treatment and the operation of the Office by Medical Group as reasonably determined by Medical Group in consultation with the Manager.

(f) No Marketing. Manager and Medical Group expressly agree and acknowledge that Manager is not being engaged to, nor at any time shall Manager, provide marketing services, directly or indirectly, to or on behalf of Medical Group.

2. Term. The term of this Agreement shall commence as of May _____, 2006 (the "Commencement Date") and, shall, unless sooner terminated as herein, continue until _____, 2031 (the "Term").

3. Provision of Professional Services. Medical Group, as an independent contractor, shall be and remain fully responsible for all professional medical services provided at the Office. In no event shall Manager be deemed to be engaged in the practice of medicine. In connection therewith, Medical Group shall provide all related physician support through its physician-employees and/or other physicians otherwise engaged by the Medical Group (the "Physicians").

4. Compensation.

(a) The Manager shall be paid, and Manager shall accept as payment for the full performance of its duties hereunder, an amount equal to seventy-seven (77%) percent of Net Collected Dollars. For purposes of this Agreement, "Net Collected Dollars" shall mean the gross collections, net of refunds, overpayments and the five percent (5%) billing fee (the "Billing Fee") due Financial Services of Southwest Florida, LLC by Medical Group pursuant to the Billing Services Agreement (as described in Section 5(a)), attributable to radiation therapy services generated by the Medical Group at the Office (the "Management Fee"). The amount of gross collections, net of refunds and overpayments and the Billing Fee, to radiation therapy services performed by the Medical Group at the Office shall be referred to herein as "Office Revenues."

(b) Payment of the Management Fee shall be due no later than the fifteenth (15th) day of the month following the last day of the month in which services were rendered by Manager hereunder.

(c) Following the expiration or other termination of this Agreement for any reason, Manager shall continue to be entitled to receive the Management Fee for services provided prior to the expiration or other termination of this Agreement but for which collections are actually received following such expiration or other termination of this Agreement.

5. Billing and Collections. Medical Group shall engage Financial Services of Southwest Florida, a Florida limited liability company to provide billing and collection services on behalf of Medical Group pursuant to that a Billing Services Agreement (the "Billing Services Agreement").

6. Representations of the Medical Group The Medical Group hereby makes the following representations, warranties and covenants to Manager, each of which shall be true as of the date hereof and shall continue to be true during the term of this Agreement:

(a) Licensed Providers. Each physician engaged by the Medical Group to provide services at the Office shall be duly licensed to practice medicine in the State of California and shall be board certified or board eligible in the specialty of radiology and shall maintain professional liability insurance in minimum amounts of \$1,000,000/\$3,000,000 per annum.

(b) Permits. Each of the Medical Group and each physician providing services on behalf of the Medical Group shall have all necessary licenses, certificates, permits, approvals, franchises, notices and authorizations issued by governmental entities or other regulatory authorities, federal, state or local, required for the ownership and operation of the Medical Group and the operation of the Practice.

(c) No Encumbrances. Title to the Equipment and other property provided by Manager hereunder shall remain with Manager. The Medical Group shall not take any action which would adversely affect or encumber Manager's title or interest in the Equipment.

(i) Responsibility for Medical Services. The Medical Group shall be and remain fully responsible for all medical services provided at the Office. In no event shall Manager be deemed to be engaged in the practice of medicine.

(d) Duly Authorized. This Agreement has been duly authorized, executed and delivered by the Medical Group and is binding upon.

(e) Duly Organized. The Medical Group is duly organized under the laws of the State of California and authorized and qualified to do all things required of it under this Agreement.

(f) Capacity to Contract. The Medical Group has the capacity and authority to fulfill the obligations required of it hereunder and nothing prohibits or restricts the right or ability of the Medical Group to carry out the terms hereof.

(g) Violations of Law. Neither the Medical Group nor any agreement, document or instrument executed or to be executed by it in connection with this Agreement, or anything provided in or contemplated by this Agreement, does or will violate any applicable law, rule or regulation or breach, invalidate, cancel, make inoperative or interfere with, or result in acceleration of maturity of, any contract or agreement to which the Medical Group is bound which would affect Manager's rights hereunder.

7. Manager's Representations. Manager hereby makes the following representations, warranties, and covenants to the Medical Group, each of which shall be true as of the date hereof and shall continue to be true during the term of this Agreement:

(a) Duly Authorized. This Agreement has been duly authorized, executed and delivered by Manager and is binding upon it;

(b) Duly Organized. Manager is duly organized under the laws of the State of California and authorized and qualified to do all things required of it under this Agreement;

(c) Capacity to Contract. Manager has the capacity and authority to fulfill the obligations required of it hereunder and, to the best of Manager's knowledge and belief, nothing prohibits or restricts the right or ability of Manager to carry out the terms hereof; and

(d) Violations of Law. Neither Manager nor any agreement, document or instrument executed or to be executed in connection with this Agreement, or anything provided in or contemplated by this Agreement, does or will, to the best of Manager's knowledge and belief, violate any applicable law, rule or regulation or breach, invalidate, cancel, make inoperative or interfere with, or result in acceleration of maturity of, any contract or agreement to which Manager is bound which would affect the rights of the Medical Group hereunder.

8. Operation of Office. In the performance of their respective obligations hereunder, Medical Group and Manager shall comply with all applicable regulations and laws (including, without limitation, applicable zoning regulations and rules and regulations governing the practice of medicine) and shall use commercially reasonable efforts to ensure that the Office complies with the rules and regulations of all regulatory bodies, agencies or authorities having jurisdiction over them.

9. Independent Contractors.

(a) This Agreement is by and between Manager and Medical Group and is not intended, and shall not be construed, to create an employment relationship, partnership or other such association as between the parties. Each party is an independent contractor of the other.

(b) Neither Manager nor its employees or agents shall look to Medical Group for vacation pay, sick leave, retirement benefits, Social Security, worker's compensation, disability or unemployment insurance benefits, or other employee benefits; nor shall Medical Group or its employees or agents look to Manager for the same.

(c) In performing the services required hereunder, Medical Group and its physician-employees and contractors shall exercise independent professional judgment. Manager shall not exercise any control over matters of Medical Group involving the exercise of professional medical judgment.

(d) In the event the Internal Revenue Service or any other governmental agency shall, at any time, question or challenge the independent contractor status of either party, the party who received notice of same shall promptly notify the other party and afford the other party the opportunity to participate in any discussion or negotiation with the Internal Revenue Service or other governmental agency, irrespective of by whom such discussions or negotiations are initiated. The other party shall participate in any such discussions or negotiations to the extent permitted by the Internal Revenue Service or other governmental agency.

(e) During the Term of this Agreement, all medical records with respect to Medical Group's patients shall remain in the custody and control of Medical Group. Such records shall be stored at such location or locations as Medical Group shall direct. Upon any

termination of this Agreement, Medical Group, at its own expense, shall remove such records from such location or locations. Notwithstanding the foregoing, at all times during the term of this Agreement and thereafter, the Manager shall be provided with access to such records, as requested, for billing and all other reasonable purposes, subject to applicable law regarding confidentiality. Manager's rights set forth in this Section 9(e) shall expressly survive any termination of this Agreement.

10. Default by Medical Group.

(a) The occurrence of any one of the following shall constitute a default by Medical Group hereunder:

- (i) if Medical Group fails to pay the Management Fee when due;
- (ii) if Medical Group is in breach of the Sublease and such breach is not cured within the applicable period provided therein;
- (iii) if Medical Group is deemed to be in breach of any of the material representations, warranties or covenants of this Agreement and such breach remains uncured for a period of thirty (30) days after delivery of written notice thereof to Medical Group from Manager, or, if such breach cannot be cured within thirty (30) days, Medical Group has failed to commence to cure such breach within such thirty (30) day period and diligently proceeded to effect such cure;
- (iv) if Medical Group fails to observe or perform any of its other obligations hereunder in any material respect and such failure continues uncured for a period of thirty (30) days after delivery of written notice thereof to Medical Group from Manager or, if such failure cannot be cured within such thirty (30) day period, Medical Group has failed to commence to cure such failure within such thirty (30) day period and diligently proceeded to effect such cure;
- (v) if Medical Group (A) ceases to practice medicine, in the specialty of radiation therapy; (B) makes an assignment for the benefit of creditors; (C) admits in writing its inability to pay its debts as they become due; (D) files a petition seeking reorganization, an arrangement, readjustment, or similar arrangement under any present or future statute, law or regulation; (E) files an answer admitting the material allegations of a petition filed against it in any such proceeding; or (F) consents to or acquiesces in the appointment of a trustee, receiver or liquidator of all or any substantial part of its assets or properties;
- (vi) if within sixty (60) days after the commencement of any proceedings against Medical Group seeking reorganization or similar relief under any present or future statute, law or regulation, such proceedings shall have not been dismissed, or if within sixty (60) days after the appointment (without Medical Group's consent or acquiescence) of any trustee, receiver or liquidator of all or any substantial part of its assets or properties, such appointment shall not have been vacated; or
- (vii) if Medical Group is determined, by an appropriate governing body or court, to have violated any applicable law, rule, regulation or ethical standard related to the

conduct of the practice of medicine which results in Medical Group being unable to provide professional medical services.

(b) Upon a default by Medical Group which has not been cured within the applicable cure period, Manager shall have the right to immediately terminate this Agreement.

11. Default by Manager.

(a) The occurrence of any one of the following shall constitute a default by Manager hereunder.

(i) If Manager fails to observe or perform any of its obligations hereunder in any material respect and such failure continues uncured for a period of thirty (30) days after written notice thereof to Manager from Medical Group or, if such failure cannot be cured within such thirty (30) day period, the Manager has failed to commence to cure such failure within such thirty (30) day period and diligently proceed to effect such cure;

(ii) If Manager: (A) makes an assignment for the benefit of creditors; (B) admits in writing its inability to pay its debt as they become due; (C) files a petition seeking reorganization and arrangement, readjustment or similar arrangement under the present or future statute, law or regulation, if any present or future; (D) files an answer admitting the material allegations of a petition filed against it and any such proceeding; or (E) consents to or acquiesces in the appointment of a trustee, receiver, or liquidator of all or any part of its assets or properties; or

(iii) If, within sixty (60) days after the commencement of any proceedings against Manager seeking reorganization or similar relief under any present or future statute, law or regulation, such proceedings shall have not been dismissed, or if within sixty (60) days after the appointment (without Manager's consent or acquiescence) of any trustee, receiver or liquidator of all or any substantial part of its assets or properties, such appointment shall not have been vacated.

(b) Upon a default by Manager, which has not been cured within the applicable cure period, Medical Group shall have the right to immediately terminate this Agreement.

12. Termination.

(a) This Agreement shall terminate upon the following events:

- (i) the mutual written agreement of the parties; or
- (ii) as provided in Sections 2, 10 and/or 11.

13. Restrictive Covenants.

(a) At all times while this Agreement remains in effect Medical Group agrees that it shall not, directly or indirectly:

(i) engage in the ownership, operation or management of any radiation oncology practice or facilities or otherwise engage in the provision of radiation oncology services (whether as a separate business or in conjunction with any other business (a "Competing Business") within an eight (8) mile radius of the Office (the "Service Area"); or

(ii) have any interest, whether as owner, stockholder, partner, member, director, officer, employee or consultant in any Competing Business in the Service Area.

(b) At all times while this Agreement remains in effect Medical Group agrees that it shall not, directly or indirectly, (i) solicit, encourage or advise patients serviced during the term of this Agreement to obtain or seek professional services from any professional who is not an employee, independent contractor or partner of Medical Group, or (ii) solicit, encourage or advise any employees of Manager to terminate employment with Manager for any reason whatsoever. Notwithstanding the foregoing, nothing in this Agreement is intended to prevent Medical Group from referring a patient in need of specialty services not otherwise provided by Medical Group, or for other reasons in the best interests of the patient, to another duly licensed professional or facility.

(c) Medical Group acknowledges that the restrictive covenants contained in this Section 13 have unique value to Manager, the breach of which cannot be adequately compensated in an action of law. Medical Group further agrees that, in the event of the breach of the restrictive covenants contained herein, Manager shall be entitled to obtain appropriate equitable relief, including, without limitation, a permanent injunction or similar court order enjoining either or both of them from violating any of such provisions, and that pending the hearing and the decision on the application for permanent equitable relief, Manager shall be entitled to a temporary restraining order and a preliminary injunction. The prevailing party shall be entitled to reimbursement from the other party of its reasonable costs and expenses (including attorneys' fees and disbursements) of, or related to, such action or proceeding. No such remedy shall be construed to be the exclusive remedy of Manager and any and all such remedies shall be held and construed to be cumulative and not exclusive of any rights or remedies, whether at law or in equity, otherwise available under the terms of this Agreement, at common law, or under federal, state or local statutes, rules and regulations.

(d) If any court of competent jurisdiction shall deem any of the restrictive covenants contained in this Section 13, or portion of any such covenants, too extensive or unenforceable, the other provisions of this Section 13 shall nevertheless stand and remain enforceable according to their terms. In such circumstance, the parties hereto expressly authorize the court to modify such covenants or offending portion thereof, so that the restrictions, limitations and scope of the restrictive covenants extend for the longest period, comprise the largest territory and are enforceable to the maximum permissible extent by law under the circumstances.

14. Confidentiality. The terms and conditions of this Agreement are and shall be treated as confidential, and shall not hereafter be disclosed by any party hereto or any of their respective attorneys to any person or entity, except to financial and legal advisors and others who need to know them to effectuate the purposes of this Agreement, or as may be required by law.

Any individual to whom the terms and conditions of this Agreement have been disclosed will be advised of and shall abide by the confidentiality instructions of this Section 14.

15. Regulatory Matters.

(a) The parties hereto acknowledge and agree that the amounts due to Manager from Medical Group pursuant to this Agreement have been determined by the parties through good faith and arm's length bargaining to be commercially reasonable, to reflect fair market value and to not in any way be based upon the volume or value of patient referrals or any other business generated between the parties. Manager and Medical Group enter into this Agreement with the intent of conducting their relationship and implementing the agreements contained in this Agreement in full compliance with applicable federal, state and local law, including without limitation, the Medicare/Medicaid Anti-Kickback statute (the "Anti-Kickback Law") and Section 1877 of the Social Security Act (the "Stark Law"), as amended. Notwithstanding any unanticipated effect of any of the provisions of this Agreement, neither party will intentionally conduct itself under the terms of this Agreement in a manner that would constitute a violation of the Anti-Kickback Law or the Stark Law or any similar California law, rule or regulation. Without limiting the generality of the foregoing, Manager and Medical Group expressly agree that nothing contained in this Agreement shall require either party to refer any patients to the other, or to any affiliate or subsidiary of the other.

(b) For purposes of this Section 15, "protected health information", or PHI, has the meaning defined by the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Subparts A and E of Part 164 (the "Privacy Standards"), as promulgated by the Department of Health and Human Services ("HHS") pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Medical Group agrees to implement appropriate administrative, technical and physical safeguards to limit incidental disclosures of PHI.

(c) Change of Law. In the event that any law, rule, regulation applicable to this Agreement or any rule or policy of any third-party payor, or any policy, or any interpretation thereof at any time during the term of this Agreement is modified, implemented, threatened to be implemented, or determined to prohibit, restrict or in any way materially change the terms of this Agreement, or by virtue of the existence of this Agreement has or will have a material adverse affect on the ability of either party to this Agreement to engage in any commercial activity on terms at least as favorable to that party as those reasonably attributable as of the date hereof (each of the foregoing being referred to herein as a "Change"), then the parties to this Agreement shall negotiate in good faith to amend this Agreement to the minimum degree necessary in a manner consistent with such change and the intent of the parties. If the parties are unable to reach agreement as to any such amendment reasonably necessary to remove the jeopardy contemplated herein, within sixty (60) days, this Agreement shall thereafter automatically terminate.

16. Miscellaneous.

(a) Notices. Any notice or other communication required or which may be given hereunder shall be in writing and shall be delivered personally, sent by certified mail, postage prepaid, return receipt requested or by a nationally recognized overnight courier, and

shall be deemed given when so delivered personally or by facsimile, or if mailed, five (5) days after the date of mailing as follows:

If to Manager:

LHA Inc.
2428 Santa Monica Boulevard, Suite 103
Santa Monica, California 90404
Attention: Michael L. Steinberg, M.D. and
Leopold T. Avallone, M.D.

If to Medical Group:

21st Century Oncology of California
2234 Colonial Boulevard
Fort Myers, Florida 33907
Attention: Daniel Dosoretz, M.D.
President and Chief Executive Officer

or to such other address and to the attention of such other person(s) or officer(s) as either party may designate by written notice.

(b) Governing Law. This Agreement shall be governed and construed in accordance with the laws of the State of California without regard to principles of conflicts of law.

(c) Further Instruments. At any time and from time to time, each party shall, without further consideration and at its own expense, take such further actions and execute and deliver such further instruments as may be reasonably necessary to effectuate the purposes of this Agreement.

(d) Entire Agreement. This Agreement (including the exhibits hereto) contains the entire understanding between the parties hereto with respect to the transactions contemplated hereby and supersedes all prior agreements between them, written or oral.

(e) Severability. In the event that any term or provision of this Agreement is held to be illegal, invalid or unenforceable under any applicable law, rule or regulation, such term or provision shall be deemed severed from this Agreement and the remaining terms and provisions shall remain unaffected thereby provided the invalid term does not materially alter the basic purpose or intent of this Agreement.

(f) Assignment. Neither party shall assign any of its rights or obligations under this Agreement without the express, prior written consent of the other party.

(g) Waiver of Breach. No waiver of a breach of any provision of this Agreement shall be construed to be a waiver of any breach of any other provision of this Agreement or of any succeeding breach.

(h) Amendments. This Agreement shall not be changed or modified except by an instrument in writing executed by both parties hereto. Without limiting any other provision herein, in the event that rules, policies, directives and/or orders of the United States

Department of Health and Human Services or any other applicable federal, state, or local agency or third-party payor necessitate modifications or amendments to this Agreement, the parties hereto agree to so modify or amend this Agreement to conform with such rules, policies, directive and/or orders, provided they do not materially affect the duties and obligations of the parties hereunder.

(i) Attorneys' Fees. In the event of a dispute hereunder, the prevailing party shall be entitled to all of its costs incurred in connection with the disposition of such dispute, including, without limitation, reasonable attorneys' fees and costs through all trial and appellate levels and post judgment proceedings.

(j) Counterparts. This Agreement may be executed in counterparts, each of which shall be considered an original and all of which together shall constitute one and the same instrument.

[SIGNATURE PAGE TO FOLLOW]

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first set forth above.

LHA, INC.

By: Michael Steinberg
Name: Michael L. Steinberg, M.D.
Title: Chairman and Chief Financial Officer

By: Leopold Avallone
Name: Leopold T. Avallone, M.D.
Title: President

21ST CENTURY ONCOLOGY OF CALIFORNIA,
a Medical Corporation

By: _____
Name:
Title:

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first set forth above.

LHA, INC.

By: _____
Name: Michael L. Steinberg, M.D.
Title: Chairman and Chief Financial Officer

By: _____
Name: Leopold T. Avallone, M.D.
Title: President

21ST CENTURY ONCOLOGY OF CALIFORNIA,
a Medical Corporation

By: 
Name: David M. Koeninger
Title: Chief Financial Officer

EXHIBIT A
Assets

1. All tangible assets used in the provision of radiation oncology services (the "Business") located at the Office, whether owned or leased, including, without limitation, all instruments, tools, medical equipment, supplies and office equipment and all fixtures and improvements.
2. All inventories of clinical supplies and instruments, pharmaceuticals, inventory, paper goods, raw materials, finished goods, demonstration equipment, parts, packaging materials and other products, materials, or accessories related thereto that are held at, or are in transit from or to, the Office.
3. All software programs (including source and object codes and related documentation for software owned by the Manager and used in connection with or developed for support of the operations of the Business, as well as the internet web sites used by Manager with respect to the Business and the related universal record locators ("URLs") used in connection therewith.
4. All files, documents, instruments, papers, books and records relating to the Business, operations, condition of (financial or other) results of operations and assets and properties of Manager, including without limitation, patient lists, medical documentation, payor verification, mailing lists and related documentation, financial statements, tax returns and related work papers and letters from accountants, personnel records and files, budgets, ledgers, journals, computer files and programs; retrieval programs, operating data and plans and environmental studies and plans.
5. All telephone numbers, facsimile numbers, electronic addresses and passwords used in connection with the Business.
6. All intangible personal property of the Manager relating to or in connection with the Business or Assets, including, without limitation, Manager's rights to and use of the name "Santa Monica Cancer Treatment Center" and all of Manager's rights, title to and interest therein and thereunder.

Exhibit B

Data Breach Complaint

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION**

IN RE: 21st CENTURY ONCOLOGY
CUSTOMER DATA SECURITY
BREACH LITIGATION

Case No. 8:16-md-2737-MSS-AEP

MDL No. 2737

This Document Relates to All Cases

CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

	PAGE
I. INTRODUCTION	1
II. NATURE OF THE ACTION	1
III. JURISDICTION	6
IV. PARTIES	6
A. Plaintiffs.....	6
Arizona.....	6
Plaintiff Robert Russell.....	6
California	7
Plaintiff James Corbel.....	7
Plaintiff Roxanne Haatvedt.....	8
Plaintiff Veneta Delucchi.....	9
Florida.....	10
Plaintiff Carl Schmitt	10
Plaintiff Matthew Benzion.....	11
Plaintiff Kathleen LaBarge	12
Plaintiff Stacey Schwartz.....	13
Plaintiff Timothy Meulenberg	14
Plaintiff Stephen Wilbur	16
Kentucky	18
Plaintiff Jackie Griffith	18
Massachusetts	19
Plaintiff Judith Cabrera	19

New Jersey	20
Plaintiff Sharon MacDermid.....	20
Rhode Island	21
Plaintiff Steven Brehio.....	21
B. Defendants	23
V. FACTUAL ALLEGATIONS	25
A. The FBI Informed 21st Century that an Intruder Gained Unauthorized Access To Patient PII/PHI and Offered this Data for Sale on the Internet	25
[REDACTED]	
[REDACTED]	
[REDACTED]	27
[REDACTED]	
[REDACTED]	31
D. The Notification Provided by 21st Century To Plaintiffs and Class Members Was Delayed, Confusing, and Misleading.....	33
1. 21st Century’s Delayed Disclosure of the Data Breach Further Harmed Plaintiffs and Class Members	33
2. 21st Century’s Notification Was False and/or Misleading and Obscured Key Facts About the Data Breach	34
3. 21st Century’s Notification Was Confusing To Plaintiffs and Class Members	35
4. Industry Insiders Confirm That 21st Century’s Data Breach Notification Was Insufficient and Inadequate	37
E. 21st Century Acknowledged Its Duty To Keep PII/PHI Private	38
1. HIPAA Provides Guidelines on How Healthcare Providers Must Secure Patients’ Protected Health Information.....	39
2. The HITECH Act Provides Additional Guidelines on How Healthcare Providers Must Secure Patients’ Protected Health Information	42

3.	21st Century Is Subject To Other Federal and State Laws and Regulations That Provide Guidelines on the Practices It Should Have Implemented To Secure Patients' Protected Health Information	43
4.	Industry Standards Also Provide Guidelines To Healthcare Providers Regarding Best Practices For Securing Confidential Medical Information	45
F.	21st Century Was Aware of the Risk of Data Breach and the Value of the PII/PHI With Which It Was Entrusted.....	46
1.	From 2011 To 2012, 21st Century Experienced a Data Breach Involving Patient PII/PHI	46
2.	The FBI Made a Highly Publicized Warning To Healthcare Companies such as 21st Century about the Increased Risk of Cyber Attacks	47
G.	21st Century Has a Marked History of Prioritizing Profit Over Patients, Performing Unnecessary Tests on its Patients for at least Seven Years	48
H.	21st Century's Response To the Data Breach Has Been Inadequate and Is Insufficient To Address the Ongoing Risks and Harms To Plaintiffs and Class Members	51
1.	The Risk of Identity Theft Is a Major Concern To Plaintiffs and Class Members	51
2.	Compromised Social Security Numbers Have Long-Term Value To Thieves and Long-Term Consequences To Data Breach Victims.....	52
3.	Compromised Medical Information Has Even Greater Long-Term Value To Thieves and Consequences for Plaintiffs and Class Members	53
4.	Thieves Will Likely Use Plaintiffs' and Class Members' PII/PHI To Hurt Them Far Longer Than One Year	54
5.	The Consequences To Victims of Medical Identity Theft Can Be Time Consuming, Financially Devastating, and Even Life Threatening	54
6.	Many of the Affected Patients Comprise a Vulnerable Population.....	58
7.	The Remedy Offered By 21st Century Is Inadequate, and Requires Plaintiffs and Class Members To Expend Time on an Ongoing Basis To Contain their Compromised PII/PHI	59

VI. CLASS ACTION ALLEGATIONS	61
A. Nationwide Class	61
B. Statewide Subclasses	62
VII. CAUSES OF ACTION	65
COUNT I NEGLIGENCE (On Behalf of the Nationwide Class and Each of the Statewide Subclasses)	65
COUNT II NEGLIGENCE PER SE (On Behalf of the Nationwide Class and Each of the Statewide Subclasses Excluding California).....	68
COUNT III GROSS NEGLIGENCE (On Behalf of the Nationwide Class and Each of the Statewide Subclasses)	70
COUNT IV NEGLIGENT MISREPRESENTATION (On Behalf of the Nationwide Class and Each of the Statewide Subclasses)	72
COUNT V BREACH OF EXPRESS CONTRACTS (On Behalf of the Nationwide Class and Statewide Subclasses).....	74
COUNT VI BREACH OF IMPLIED CONTRACTS (On Behalf of the Nationwide Class and Statewide Subclasses).....	77
COUNT VII BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING (On Behalf of the Nationwide Class and Statewide Subclasses) ..	80
COUNT VIII BREACH OF FIDUCIARY DUTY (On Behalf of the Nationwide Class and Statewide Subclasses).....	82
COUNT IX UNJUST ENRICHMENT (Alternative To Breach of Contract Claim) (On Behalf of the Nationwide Class and Statewide Subclasses)	83
COUNT X INVASION OF PRIVACY (On Behalf of the Nationwide Class and Statewide Subclasses)	85
COUNT XI DECLARATORY JUDGMENT (On Behalf of the Nationwide Class and Statewide Subclasses)	86
COUNT XII Violations of the Arizona Consumer Fraud Act Ariz. Rev. Stat. Ann. §§ 44-1521, <i>et seq.</i> (On Behalf of the Arizona Subclass).....	87
COUNT XIII Violations of the California Confidentiality of Medical Information Act Cal. Civ. Code § 56, <i>et seq.</i> (On Behalf of the California Subclass)	92

COUNT XIV Violations of the California Unfair Competition Law Cal. Bus. & Prof. Code § 17200, <i>et seq.</i> (On Behalf of the California Subclass)	95
COUNT XV Violations of the California Customer Records Act Cal. Civ. Code § 1798.81.5, <i>et seq.</i> (On Behalf of the California Subclass).....	99
COUNT XVI Violations of the California Consumers Legal Remedies Act (“CLRA”) Cal. Civ. Code § 1750, <i>et seq.</i> (On Behalf of the California Subclass).....	102
COUNT XVII Violations of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, <i>et seq.</i> (On Behalf of the Florida Subclass)	105
COUNT XVIII Violations of the Kentucky Consumer Protection Act Ky. Rev. Stat. §§ 367.170, <i>et seq.</i> (On Behalf of the Kentucky Subclass)	109
COUNT XIX Violations of the Massachusetts Consumer Protection Act Mass. Gen. Laws Ann. Ch. 93A, § 1, <i>et seq.</i> (On Behalf of the Massachusetts Subclass)	114
COUNT XX Violations of the Massachusetts Right To Privacy Statute Mass. Gen. Laws Ann. ch. 214, § 1B. (On Behalf of the Massachusetts Subclass)	118
COUNT XXI Violations of the New Jersey Consumer Fraud Act N.J. Stat. Ann. § 56:8-1, <i>et seq.</i> (On Behalf of the New Jersey Subclass)	122
COUNT XXII Violations of the Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1, <i>et seq.</i> (On Behalf of the Rhode Island Subclass)	125
VIII. PRAYER FOR RELIEF	130
IX. JURY TRIAL DEMANDED	130

I. INTRODUCTION

Plaintiffs,¹ individually and on behalf of all others similarly situated (“Class members”), file this Consolidated Class Action Complaint against 21st Century Oncology Investments, LLC and 21st Century Oncology of California, a Medical Corporation (collectively “Defendants” or “21st Century”), and allege as follows based on personal knowledge, the investigation of their counsel, and information and belief.

II. NATURE OF THE ACTION

1. As any medical patient, survivor, or loved one can attest—and 21st Century recognizes on its website²—medical challenges are stressful and difficult, and a cancer diagnosis especially seems to place one’s life out of control:



¹ “Plaintiffs” refers collectively to Plaintiffs Matthew Benzion, Steven Brehio, Judith Cabrera, James Corbel, Veneta Delucchi, Jackie Griffith, Roxanne Haatvedt, Kathleen LaBarge, Sharon MacDermid, Timothy Meulenberg, Robert Russell, Carl Schmitt, Stacey Schwartz, and Stephen Wilbur.

² 21st Century, *What to Expect as a Cancer Patient*, <https://www.21co.com/radiation-therapy/what-to-expect> (last visited Mar. 18, 2016).

2. The last thing patients dealing with potentially deadly illnesses need is further harm and stress caused by the insecurity of their most private data and how it may be used by thieves.

3. But that is exactly what victims of a data breach at 21st Century that occurred on or around October 3, 2015 (“Data Breach”) are enduring nationwide. Millions of 21st Century Data Breach victims have lost control of sensitive information that endangers their financial, medical, and emotional well-being for the rest of their lives. Plaintiffs are Data Breach victims and bring this proposed class action lawsuit on behalf of themselves and all other persons whose personally identifiable information (“PII”) and protected health information (“PHI”) have been compromised as a result of the 21st Century Data Breach (the “Class”).

4. While more than 2.2 million 21st Century Data Breach victims sought out and/or paid for medical care from Defendants, thieves were hard at work, stealing and using their hard-to-change Social Security numbers and highly sensitive PII/PHI for over five months without the victims’ knowledge. 21st Century’s lax security practices that allowed this intrusion have worsened Plaintiffs’ and other Class members’ lives by, among other injuries: (a) adding to their already heightened financial obligations by placing them at increased risk of fraudulent charges; (b) complicating diagnosis, prognosis, and treatment for their severe medical conditions by placing them at increased risk of having inaccurate medical information in their files; and/or (c) increasing the risk of other potential personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed.

5. On or around October 3, 2015, unauthorized parties hacked into 21st Century's provider database; however, 21st Century apparently failed to detect the Data Breach until the Federal Bureau of Investigation ("FBI") notified it on or about November 13, 2015.³

6. The Data Breach resulted in the disclosure of private and highly sensitive PII/PHI including: names, Social Security numbers, physician's names, medical diagnoses, treatment information, and insurance information.⁴

7. 21st Century is not a name known to all Class members because 21st Century operates numerous facilities throughout the country under different trade names. In fact, some Class members were surprised and alarmed to learn that 21st Century—a company they were not familiar with—had access to their PII/PHI at all, much less had lost control of their PII/PHI and allowed it to be compromised by unauthorized parties who could further distribute their private and sensitive information to anyone and everyone, including identity thieves.

8. Prior to the Data Breach, 21st Century acknowledged in the Notice of Privacy Practices posted on its website that it is "required by law to maintain the privacy of your protected health information, to provide you with notice of our legal duties and privacy practices with respect to that protected health information, and to notify any affected individuals following a breach of any unsecured protected health information."⁵ 21st Century

³ 21st Century, *Notice to Patients Regarding Security Incident* (Mar. 4, 2016), <https://www.21co.com/securityincident> (last visited Mar. 18, 2016).

⁴ *Id.*

⁵ 21st Century, *Notice of Privacy Practices* (Mar. 26, 2013), <https://www.21co.com/company/hipaa-notice-of-privacy-practices> (last visited Jan. 17, 2017).

also represented that it would abide by these obligations, but failed to live up to its own promises as well as its duties and obligations required by law and industry standards.

9. Contrary to its promises to help patients improve the quality of their lives through secure data practices, 21st Century's conduct has instead been a direct cause of the ongoing harm to Plaintiffs and other Class members whose suffering has been magnified by the Data Breach, and who will continue to experience harm and data insecurity for the indefinite future.

10. Specifically, 21st Century failed to maintain reasonable and/or adequate security measures to protect Plaintiffs' and other Class members' PII/PHI from unauthorized access and disclosure, apparently lacking, at a minimum: (1) reasonable and adequate security measures designed to prevent this attack even though 21st Century suffered from at least one previous data breach, and knew or should have known that it was a prized target for hackers; and (2) reasonable and adequate security protocols to promptly detect the unauthorized intrusion into and removal of PII/PHI from its provider database pertaining to 2.2 million 21st Century Data Breach victims.

11. Moreover, while 21st Century had months to figure out how to protect and minimize harm to Plaintiffs and Class members from the Data Breach, its response was haphazard and ineffective. First, 21st Century harmed Plaintiffs and Class members through delayed notification. Adding insult to injury, it then offered only one year of credit monitoring and identity theft insurance, and provided only four months from notification of the Data Breach in which to sign up. Moreover, credit monitoring and identity theft insurance alone do not eliminate the risk of identity theft and fraud. Even with such

protections, Plaintiffs and Class members may still experience identity theft and then be required to spend significant time undoing the financial injury inflicted by identity thieves who seek to use their compromised PII/PHI for financial gain.

12. In addition, credit monitoring fails to remedy the potentially life-threatening injury to Plaintiffs and other Class members inflicted by identity thieves who seek to use victims' compromised PII/PHI to obtain medical care, thereby placing the thieves' inaccurate information on innocent victims' medical records in the process. This harm is particularly dangerous for oncology patients.

13. Thieves with access to Plaintiffs' and other Class members' compromised PII/PHI can use their Social Security numbers indefinitely because, unlike credit and financial accounts, these numbers are extremely difficult to change. In addition, medical identity theft can continue to harm Plaintiffs and other Class members indefinitely because this information is often shared amongst numerous providers. Further, as a consequence of the Data Breach, Plaintiffs and Class members are at increased risk of personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed.

14. Plaintiffs bring this proposed class action lawsuit on behalf of themselves and the Class. They seek damages, restitution, and injunctive relief requiring 21st Century to implement and maintain security practices to comply with regulations designed to prevent and remedy this and other potential data breaches, as well as other relief as the Court may order. Plaintiffs and Class members will have to remain vigilant for the rest of their lives to combat potential identity theft. Despite all best efforts of Plaintiffs, Class members, or anyone else, this most sensitive personal data can never be made private again.

III. JURISDICTION

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds \$5 million, exclusive of interest and costs, Defendants do business nationwide in 17 states, and members of the proposed class are citizens of different states than Defendants.

16. This Court has personal jurisdiction over 21st Century because 21st Century maintains its headquarters and principal executive and administrative offices in Florida and has sufficient minimum contacts with Florida.

17. Venue is proper in this district under 28 U.S.C. § 1391(b) because 21st Century resides in this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district. Venue is also appropriate in this district pursuant to United States Judicial Panel on Multidistrict Litigation's October 6, 2016 Transfer Order transferring and centralizing this case in the Middle District of Florida.

IV. PARTIES

A. Plaintiffs

Arizona

Plaintiff Robert Russell

18. Plaintiff Robert Russell is a citizen of and is domiciled in the state of Arizona. Plaintiff Russell is unable to determine how 21st Century obtained his confidential and sensitive PII/PHI.

19. In March 2016, Plaintiff Russell received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

20. Plaintiff Russell subsequently spent approximately 15 to 20 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, reviewing credit reports and financial accounts for fraud or suspicious activity, reviewing medical statements for fraud or suspicious activity, researching and enrolling in the credit monitoring service offered by 21st Century, and contacting 21st Century, a government agency, and a medical insurer regarding the Data Breach.

21. As a result of the Data Breach, Plaintiff Russell has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Russell anticipates spending considerable time and money to contain the impact of the Data Breach.

California

Plaintiff James Corbel

22. Plaintiff James Corbel is a citizen of and is domiciled in the state of California. Plaintiff Corbel received medical services from 21st Century affiliates located in California and provided confidential and sensitive PII/PHI to 21st Century.

23. In March 2016, Plaintiff Corbel received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

24. Plaintiff Corbel subsequently spent approximately 10 hours taking action to mitigate the impact of the Data Breach, including requesting and reviewing a credit report, and reviewing financial accounts for fraud or suspicious activity.

25. Despite Plaintiff Corbel's efforts to protect himself, he began receiving suspicious telephone calls asking for money and/or Plaintiff Corbel's personal information.

26. As a result of the Data Breach, Plaintiff Corbel has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Corbel anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Roxanne Haatvedt

27. Plaintiff Roxanne Haatvedt is a citizen of and is domiciled in the state of California. Plaintiff Haatvedt received medical services from an affiliate of 21st Century located in California and provided confidential and sensitive PII and PHI to Defendants.

28. In March 2016, Plaintiff Haatvedt received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

29. Plaintiff Haatvedt subsequently spent approximately 20 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, reviewing credit reports and financial accounts for fraud or suspicious activity, and researching and enrolling in the credit monitoring service offered by Defendants.

30. As a result of the Data Breach, Plaintiff Haatvedt has suffered emotional distress as a result of the release of her protected health information which she expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using her personal and medical information. As

a result of the Data Breach, Plaintiff Haatvedt anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Veneta Delucchi

31. Plaintiff Veneta Delucchi is a citizen of and is domiciled in the state of California. Plaintiff Delucchi received medical services from an affiliate of 21st Century located in California and provided confidential and sensitive PII/PHI to Defendants.

32. In March 2016, Plaintiff Delucchi received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

33. Plaintiff Delucchi subsequently spent approximately 10 to 15 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, reviewing financial accounts for fraud or suspicious activity, and researching and enrolling in the credit monitoring service offered by 21st Century.

34. When the credit monitoring service offered by 21st Century expires, Plaintiff Delucchi plans to pay for a credit monitoring service on an ongoing basis to protect herself from identity theft and fraud.

35. As a result of the Data Breach, Plaintiff Delucchi has suffered emotional distress as a result of the release of her protected health information which she expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Delucchi anticipates spending considerable time and money to contain the impact of the Data Breach.

Florida

Plaintiff Carl Schmitt

36. Plaintiff Carl Schmitt is a citizen of and is domiciled in the state of Florida. Plaintiff Schmitt received medical services from a 21st Century affiliate located in Florida, and provided confidential and sensitive PII and PHI to 21st Century.

37. In January 2016, Plaintiff Schmitt discovered that his PII had been used by unauthorized parties to commit fraud. Plaintiff Schmitt received notifications from Capital One, Amazon, and Chase that fraud was committed using his PII. For instance, Plaintiff Schmitt received notification from Capital One that the address on his account was changed and that a request was made to send replacement credit cards to the new address. Plaintiff Schmitt also received notification from Amazon that someone attempted to open an Amazon credit card in his name and they were in the process of ordering items Plaintiff Schmitt did not order. Plaintiff Schmitt blocked that account. Plaintiff Schmitt received a phishing email purporting to be Bank of America asking that he provide certain information. Plaintiff Schmitt went to Bank of America and they verified it was not an email sent by Bank of America. A new Bank of America credit card was reissued to Plaintiff Schmitt. Plaintiff Schmitt also received notification from Chase that an unauthorized parties attempted to change his contact information. A credit card had to be reissued to prevent unauthorized transactions. Plaintiff Schmitt also received numerous other phishing emails during this time period. Plaintiff Schmitt subsequently spent over approximately 60 hours taking action to mitigate the impact of the Data Breach, corresponding and communicating with Capital One, Amazon, Bank of America and Chase, confirming his financial institutions had his proper

contact information, reviewing financial accounts for fraud or suspicious activities, contacting the FTC and the local police departments to report the fraudulent activity, and placing credit freezes with Experian, Equifax and TransUnion.

38. In April 2016, Plaintiff Schmitt received notice from 21st Century that his PII and PHI had been compromised in the Data Breach.

39. Plaintiff Schmitt subsequently spent additional time taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st Century, and researching ways to protect himself from data breaches.

40. As a result of the Data Breach, Plaintiff Schmitt has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Schmitt anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Matthew Benzion

41. Plaintiff Matthew Benzion is a citizen of and is domiciled in the state of Florida. Plaintiff Benzion received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to 21st Century.

42. In March 2016, Plaintiff Benzion received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

43. Plaintiff Benzion subsequently spent approximately 15 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and 21st

Century, researching ways to protect himself from data breaches, reviewing his financial accounts for fraud or suspicious activity, and enrolling in a credit monitoring service.

44. As a result of the Data Breach, Plaintiff Benzion purchased LifeLock Ultimate Plus, a credit monitoring service, for which he pays \$29.99 per month.

45. As a result of the Data Breach, Plaintiff Benzion has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Benzion anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Kathleen LaBarge

46. Plaintiff Kathleen LaBarge is a citizen of and is domiciled in the state of Florida. Plaintiff LaBarge received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to Defendants.

47. In March 2016, Plaintiff LaBarge received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

48. Plaintiff LaBarge has spent \$99.00 to obtain identity theft protection with LifeLock.

49. As a result of the Data Breach, Plaintiff LaBarge has suffered emotional distress as a result of the release of her protected health information which she expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using her personal and medical information. As

a result of the Data Breach, Plaintiff LaBarge anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Stacey Schwartz

50. Plaintiff Stacey Schwartz is a citizen of and is domiciled in the state of Florida. He received medical services from an affiliate of Defendants located in Florida and provided confidential and sensitive PII/PHI to Defendants.

51. In March 2016, Plaintiff Schwartz received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

52. After receiving notice about the Data Breach, Plaintiff Schwartz spent approximately 13 hours taking action to mitigate the impact of the Data Breach, including (a) researching the Data Breach and Defendants; (b) contacting Defendants to inquire about the Data Breach and to confirm that the notice he received was not a scam; (c) researching and ultimately enrolling in credit monitoring services with LifeLock, for which he pays \$197.90 annually; and (d) reviewing his financial accounts for fraud or suspicious activity.

53. Despite Plaintiff Schwartz's efforts to protect himself, he discovered that his PII has been used by unauthorized parties to commit fraud. On April 25, 2016, Plaintiff Schwartz received an alert from LifeLock notifying him that an unknown third party had used his name, date of birth, and Social Security number to apply for a Capital One credit card. He informed LifeLock and Capital One that he did not submit this application. On September 30, October 1, and October 2, 2016, Plaintiff Schwartz received three separate notifications from Chase that on August 1, an unknown third party had attempted to apply for a Chase credit card using his PII. Plaintiff Schwartz has spent approximately an additional

16 hours addressing the fraudulent activity, including (a) contacting LifeLock, Capital One, and Chase to inform them that he did not submit credit card applications; (b) filing a police report with the Miami police; (c) filing an online complaint with the Federal Bureau of Investigation; (d) contacting financial institutions with which he does business to add protection to his accounts and to discuss other options to protect himself and his accounts; (e) placing security freezes on his credit with Experian, Equifax, and TransUnion, for which he paid \$30.00; and (f) filing a complaint with the FTC.

54. As a result of the Data Breach, Plaintiff Schwartz has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Schwartz anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Timothy Meulenberg

55. Plaintiff Timothy Meulenberg, is a citizen of and is domiciled in the state of Florida. Plaintiff Meulenberg received medical services from Defendants located in Florida and provided confidential and sensitive PII/PHI to Defendants.

56. In March 2016, Plaintiff Meulenberg received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

57. Plaintiff Meulenberg subsequently spent approximately 16 hours taking action to mitigate the impact of the Data Breach, including contacting credit card companies, the

three major credit reporting agencies, the Social Security Administration, and the Internal Revenue Service.

58. Plaintiff Meulenberg has also spent \$30.00 to place credit freezes on his accounts with each of the three major credit-reporting agencies.

59. Despite Plaintiff Meulenberg's efforts to protect himself, he discovered that his PII had been used by unauthorized parties to commit fraud. On February 24, 2016, an attempt was made by an unauthorized parties to open a Bank of America credit card account. Furthermore, on March 10, 2016, an attempt was made by an unauthorized parties to open a Discover credit card account. Also, on or about November 2016, Plaintiff Meulenberg discovered unauthorized charges totaling \$170.00 on his Fifth Third Bank credit card account. Plaintiff Meulenberg has spent approximately 25 hours addressing the fraudulent activities, including contacting the credit card companies involved and the three major credit reporting agencies.

60. As a result of the Data Breach, Plaintiff Meulenberg has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Meulenberg anticipates spending considerable time and money to contain the impact of the Data Breach.

Plaintiff Stephen Wilbur

61. Plaintiff Stephen Wilbur is a citizen of and is domiciled in the state of Florida.

Plaintiff Wilbur received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to Defendants.

62. In January 2016, when Plaintiff Wilbur's wife attempted to pick up Plaintiff Wilbur's prescription, a Walgreens pharmacist informed her that Plaintiff Wilbur's health insurance coverage was not valid. Plaintiff Wilbur contacted his health insurance company to determine why his health insurance was invalid, and a representative informed him that it had been cancelled and that the company would commence an investigation. Plaintiff Wilbur learned through his health insurance agent that his Social Security number had been compromised. Because his Social Security number had been stolen, Plaintiff Wilbur's health insurance company was unable to reinstate his coverage under his Social Security number and had to create a fictitious Social Security number to create a new health insurance account under his name.

63. During the time he was without coverage, Plaintiff Wilbur's health insurance company denied his claims for medical services. As a result, he incurred out-of-pocket costs of over \$575.00. Additional out-of-pocket costs were only recouped after extensive delay and effort by Plaintiff Wilbur and his wife.

64. In March 2016, Plaintiff Wilbur received notice from 21st Century that his PII/PHI had been compromised in the Data Breach.

65. In November or December 2016, Plaintiff Wilbur received notice from the health insurance company that the Internal Revenue Service had rejected his fictitious

number. Plaintiff Wilbur may be liable for tax penalties for “failure” to have health insurance coverage, for which Plaintiff Wilbur has had to provide proof. The Internal Revenue Service investigation is pending. On January 11, 2017, Plaintiff Wilbur’s health insurance company informed him that it would notify the Social Security Administration that his Social Security number has been stolen.

66. Plaintiff Wilbur has spent approximately 75 to 80 hours addressing the fraudulent activity, including (a) contacting his health insurance company regarding the fraud; (b) communicating with his health insurance agent and attempting to reinstate his health insurance coverage; (c) searching for and obtaining alternative health insurance coverage that provides him less favorable and more expensive coverage; and (d) corresponding with the Internal Revenue Service regarding his health insurance coverage.

67. After receiving notice about the Data Breach, Plaintiff Wilbur spent 75 to 80 hours taking action to mitigate further impact of the Data Breach, including (a) researching the Data Breach and Defendants; (b) attempting to contact Defendants to inquire about the Data Breach to which Defendants have been unresponsive; (c) enrolling in credit monitoring services; (d) reviewing his credit report and financial accounts for fraud or suspicious activity; (e) filing a complaint online with the FTC; and (f) notifying his Certified Public Accountant of the Data Breach.

68. As a result of the Data Breach, Plaintiff Wilbur has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As

a result of the Data Breach, Plaintiff Wilbur anticipates spending considerable additional time and money to contain and try to mitigate further impact of the Data Breach.

Kentucky

Plaintiff Jackie Griffith

69. Plaintiff Jackie Griffith is a citizen of and is domiciled in the state of Kentucky. Plaintiff Griffith received medical services from a 21st Century affiliate located in Kentucky and provided confidential and sensitive PII/PHI to Defendants.

70. In March 2016, Plaintiff Griffith received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

71. Plaintiff Griffith subsequently spent approximately an hour or two every month taking action to mitigate the impact of the Data Breach, including investigating a possible fraudulent charge placed on Amazon in her name, reviewing credit reports and/or financial accounts for fraud or suspicious activity, and enrolling in credit monitoring services with Experian. In late March of 2016, Plaintiff Griffith was notified by PNC Bank that an unauthorized user attempted to access her credit card. As a result, she had to spend time on the phone with the bank and changing her password.

72. Despite Plaintiff Griffith's efforts to protect herself, she discovered that her PII had been used by unauthorized parties to commit or attempt to commit fraud in 2016 when she received email notifications of possible fraudulent purchases made in her name on Amazon. Plaintiff Griffith knew this was suspicious because she had never shopped at Amazon, and she spent time on the phone with them attempting to remedy and prevent fraudulent purchases. Plaintiff Griffith has spent and continues to spend an hour or two each

month addressing the threat of fraudulent activity, including investigating the potentially fraudulent charges on Amazon, investigating and responding to attempts of unauthorized usage of her PNC credit card, disputing an attempt by a Tennessee collection agency to put a false Tennessee address on her credit report, resulting in a “hold” on her credit, and enrolling in credit monitoring services with Experian.

73. As a result of the Data Breach, Plaintiff Griffith has suffered emotional distress as a result of the release of her protected health information which she expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Griffith anticipates spending considerable time and money to contain the further impact of the Data Breach.

Massachusetts

Plaintiff Judith Cabrera

74. Plaintiff Judith Cabrera is a citizen of and is domiciled in the Commonwealth of Massachusetts. She received medical services from a 21st Century affiliate located in Florida and provided confidential and sensitive PII/PHI to Defendants.

75. In March 2016, Plaintiff Cabrera received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

76. After receiving notice about the Data Breach, Plaintiff Cabrera spent approximately 50 hours taking action to mitigate the impact of the Data Breach, including (a) researching the Data Breach; (b) reviewing her financial account and credit score daily for fraud or suspicious activity; (c) attempting to enroll in the free credit monitoring services

offered in the Data Breach notice and finding that the services were no longer available; and (d) researching and ultimately enrolling in credit monitoring services with LifeLock, for which she pays \$186.91 annually.

77. Despite Plaintiff Cabrera's efforts to protect herself, she discovered that her PII has been sold or traded by unauthorized parties. On January 15, 2017, Plaintiff Cabrera received an alert from LifeLock notifying her that her PII has been "given away, traded or sold" on the "Dark Web, Deep Web, or Peer-to-Peer File Sharing Networks."

78. As a result of the Data Breach, Plaintiff Cabrera has suffered emotional distress as a result of the release of her protected health information which she expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff Cabrera anticipates spending considerable time and money to contain the impact of the Data Breach.

New Jersey

Plaintiff Sharon MacDermid

79. Plaintiff Sharon MacDermid is a citizen of and is domiciled in the state of New Jersey. Plaintiff MacDermid received medical services from a division of 21st Century located in Florida and provided confidential and sensitive PII/PHI to Defendants.

80. In March 2016, Plaintiff MacDermid received notice from 21st Century that her PII/PHI had been compromised in the Data Breach.

81. Plaintiff MacDermid subsequently spent approximately 10 to 15 hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach and

21st Century, reviewing financial accounts for fraud or suspicious activity, and researching how to protect herself from the consequences of the Data Breach.

82. Plaintiff MacDermid pays \$12.99 per month for credit monitoring and identity theft protection services by Bank of America Privacy Assist, and plans to continue paying for these services once the period during which 21st Century is offering credit monitoring services to Data Breach victims expires.

83. As a result of the Data Breach, Plaintiff MacDermid has suffered emotional distress as a result of the release of her protected health information which she expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using her personal and medical information. As a result of the Data Breach, Plaintiff MacDermid anticipates spending considerable time and money to contain the impact of the Data Breach.

Rhode Island

Plaintiff Steven Brehio

84. Plaintiff Steven Brehio is a citizen of and is domiciled in the state of Rhode Island. Plaintiff Brehio received medical services from an affiliate of 21st Century Oncology located in Rhode Island and provided confidential and sensitive PII/PHI to 21st Century.

85. In March 2016, Plaintiff Brehio received notice from 21st Century that his PII/PHI had been compromised in the Data Breach. After learning of the Data Breach, Plaintiff Brehio enrolled in the one-year membership with Experian's ProtectMyID Alert offered by 21st Century.

86. Despite Plaintiff Brehio's efforts to protect himself from fraud following the Data Breach, he discovered that his PII had been used by unauthorized parties to commit fraud. Plaintiff Brehio was notified in approximately July 2016 by AT&T that an account for two cell phones was opened in his name. Plaintiff Brehio received a bill from AT&T for \$282.83. Plaintiff Brehio was also notified in approximately July 2016 by eBay that his account was used fraudulently without his permission. Plaintiff Brehio was notified in approximately August 2016 that someone was using his name, Social Security number and date of birth to try to open a Target credit card account in his name. Plaintiff Brehio has spent approximately 10 hours addressing the fraudulent activity, including contacting AT&T and Target, filing reports with local police agencies and the Federal Trade Commission, reviewing his accounts and placing credit freezes with Experian, Equifax and TransUnion.

87. Plaintiff Brehio spent approximately 20 hours taking action to mitigate the impact of the Data Breach, including researching 21st Century and the Data Breach, reviewing financial accounts for fraudulent or suspicious activity, researching and enrolling in the credit monitoring service offered by 21st Century, contacting local police agencies and the FTC regarding fraudulent activities and placing credit freezes with Experian, Equifax and TransUnion.

88. Plaintiff Brehio has also spent approximately \$20.00 in mileage to provide information to local police agencies about the fraudulent activities on his accounts. As a result of the Data Breach, Plaintiff Brehio intends to purchase additional credit monitoring services once the Experian ProtectMyID service expires.

89. As a result of the Data Breach, Plaintiff Brehio has suffered emotional distress as a result of the release of his protected health information which he expected 21st Century to protect from disclosure, including anxiety, concern and unease about unauthorized parties viewing and potentially using his personal and medical information. As a result of the Data Breach, Plaintiff Brehio anticipates spending considerable time and money to contain the impact of the Data Breach. This includes weekly checks of personal and financial accounts and the extension of his credit freeze for seven years.

B. Defendants

90. Defendant 21st Century Oncology Investments, LLC is a Delaware limited liability company with its principal place of business in Ft. Myers, Florida. Defendant 21st Century Oncology Investments, LLC is the 100% owner of its subsidiary 21st Century Oncology Holdings, Inc., which in turn is the 100% owner of its subsidiary 21st Century Oncology, Inc., which in turn is the 100% owner of its subsidiaries 21st Century Oncology, LLC, 21st Century Oncology Management Services, Inc., and 21st Century Oncology Services, LLC.

91. Defendant 21st Century Oncology of California, a Medical Corporation, is a California corporation with its principal place of business in Florida. Defendant 21st Century Oncology of California, a Medical Corporation, is an affiliated professional corporation/association of 21st Century Oncology, Inc., which in turn is a subsidiary that is 100% owned by 21st Century Oncology Investments, LLC.

92. 21st Century Oncology Investments, LLC and 21st Century Oncology of California, a Medical Corporation (collectively “Defendants” or “21st Century”) comprise a

global, physician-led provider of integrated cancer care services, which bills itself as “the premier provider of cancer care services across multiple modalities.”⁶ 21st Century claims to be the largest radiation oncology provider in the United States.

93. Defendants provide a full spectrum of cancer care services by employing and affiliating with physicians in their related specialties, which enables 21st Century to collaborate across its physician base, integrate services and payments for related medical needs, and disseminate its medical practices on a broad scale.

94. Defendants operate the largest integrated network of cancer treatment centers and affiliated physicians in the world. 21st Century operates in more than 500 locations in the United States, and employs or is affiliated with over 800 physicians, including medical oncologists, radiation oncologists, and other specialists that include urologists, hematologists, gynecologic oncologists, surgeons, and pathologists. 21st Century advertises that it maintains specialties in a number of cancer-related treatments and surgeries, including those such as radiation oncology, breast cancer surgery, colorectal surgery, gynecological surgery, general surgery, urology, pulmonology, and primary care, among others.

95. Defendants’ cancer treatment centers in the United States are operated predominantly under the *21st Century Oncology* brand and are located in 17 states: Alabama, Arizona, California, Florida, Indiana, Kentucky, Maryland, Massachusetts, Michigan, Nevada, New Jersey, New York, North Carolina, Rhode Island, South Carolina, Washington and West Virginia. 21st Century also manages 36 treatment centers in seven countries in Latin America.

⁶ 21st Century Oncology, *Corporate Overview*, <https://www.21co.com/overview> (last visited Jan. 6, 2017).

V. FACTUAL ALLEGATIONS

A. The FBI Informed 21st Century that an Intruder Gained Unauthorized Access To Patient PII/PHI and Offered this Data for Sale on the Internet

96. On November 13, 2015, the FBI advised 21st Century that “patient information was illegally obtained by a third party who may have gained access to a 21st Century database.”⁷

Term	Percentage
GMOs	85%
Organic	82%
Natural	78%
Artificial	65%
GMOs	85%
Organic	82%
Natural	78%
Artificial	65%
GMOs	85%
Organic	82%
Natural	78%
Artificial	65%
GMOs	85%
Organic	82%
Natural	78%
Artificial	65%

⁷ 21st Century, *Letter to Office of the Attorney General of New Hampshire* (Mar. 4, 2016) (hereinafter “NH Notification Letter”), <http://doj.nh.gov/consumer/security-breaches/documents/21st-century-oncology-20160304.pdf>.

A horizontal bar chart consisting of 15 black bars of varying lengths. The bars are arranged vertically from top to bottom. The lengths of the bars decrease from top to bottom, with the shortest bar at the bottom. There are small black squares at the start and end of the first bar, and a small black square at the start of the second bar.

The figure consists of 15 horizontal bars of varying lengths and positions. The bars are black and are set against a white background. The lengths of the bars range from approximately 10% to 100% of the total width. The positions of the bars are scattered across the page, with some appearing near the top and others near the bottom. A legend is located at the bottom left, featuring a horizontal line and three small black squares of increasing size.

Figure 1: A series of 15 horizontal bars, each consisting of a short black segment on the left and a long black segment on the right. The bars are evenly spaced vertically. The first bar has a small white square at its left end. The second bar has a small white square at its left end. The third bar has a small white square at its left end. The fourth bar has a small white square at its left end. The fifth bar has a small white square at its left end. The sixth bar has a small white square at its left end. The seventh bar has a small white square at its left end. The eighth bar has a small white square at its left end. The ninth bar has a small white square at its left end. The tenth bar has a small white square at its left end. The eleventh bar has a small white square at its left end. The twelfth bar has a small white square at its left end. The thirteenth bar has a small white square at its left end. The fourteenth bar has a small white square at its left end. The fifteenth bar has a small white square at its left end.

Term	Percentage
GMOs	~10%
Organic	~85%
Natural	~75%
Artificial	~65%
Organic	~85%
Natural	~75%
Artificial	~65%
Organic	~85%
Natural	~75%
Artificial	~65%

Term	Percentage (%)
Organic	100
Natural	100
Non-GMO	75
Artificial	100
Chemical	100
Genetically modified	100
Organic	100
Natural	100
Non-GMO	75
Artificial	100
Chemical	100
Genetically modified	100
Organic	100
Natural	100
Non-GMO	75
Artificial	100
Chemical	100
Genetically modified	100

A horizontal bar chart with seven categories on the x-axis and seven bars on the y-axis. The bars are black and of varying lengths. The categories are represented by small black squares to the left of the bars.

Category	Count
1	2
2	3
3	5
4	6
5	2
6	3
7	2

A horizontal bar chart consisting of 15 bars. The first 14 bars are solid black and extend to the right. The 15th bar is a shorter, lighter gray bar located at the bottom left. The bars are arranged vertically from top to bottom.

D. The Notification Provided by 21st Century To Plaintiffs and Class Members Was Delayed, Confusing, and Misleading

1. 21st Century's Delayed Disclosure of the Data Breach Further Harmed Plaintiffs and Class Members

117. Despite the risk to its patients of fraud and other identity theft, 21st Century delayed notifying patients of the Data Breach until March 4, 2016, almost four months after it was informed of the Data Breach.⁴⁰ Although Defendants claim that “[t]he FBI asked 21st Century to delay notification or public announcement of the incident until now so as not to interfere with its investigation,” Defendants have not provided evidence of such a request or an explanation of how such a request would relieve 21st Century of its notification obligations.⁴¹

118. In the intervening months between when the FBI notified 21st Century of the Data Breach and when 21st Century disclosed it to Plaintiffs and Class members, 21st Century focused **not** on protecting patients and others whose PII/PHI it collected, retained, and compromised through its lax security measures, but rather on controlling the damage to itself and its investors.

119. During the four months during which 21st Century failed to notify Plaintiffs and Class members of the Data Breach—Plaintiffs and Class members were at an especially heightened risk of identity theft. Not only was their most sensitive PII/PHI already for sale on the internet without their knowledge, but this period overlapped with months during which income tax returns are filed, putting them at an increased risk of tax fraud.

⁴⁰ See *supra*, NH Notification Letter.

⁴¹ *Id.*

120. For this reason, many Class members were blindsided by the notification that their Social Security numbers were compromised with only weeks remaining before the tax-filing deadline. Further, many Class members found activating the credit monitoring service to be confusing and time consuming, thereby increasing the stress and anxiety associated with the uncertainty about whether that the Data Breach would jeopardize any expected tax refunds.

2. 21st Century's Notification Was False and/or Misleading and Obscured Key Facts About the Data Breach

121. Despite having had months to prepare its notification to Plaintiffs and Class members, the March 4, 2016 notification letter sent by 21st Century indicates only that, “on October 3, 2015, [an] intruder *may* have accessed [a] database, which contained information that *may* have included your name, Social Security number, physician’s name, diagnosis and treatment information, and insurance information”⁴² Further, 21st Century represented to Plaintiffs and Class members that “[w]e have no evidence that your medical record was accessed,” and “[w]e have no indication that your information has been misused in any way.”⁴³

122. As is indicated above, this notification was false and/or misled Plaintiffs and Class members by inaccurately conveying that 21st Century did not possess information that patient medical information had, in fact, been improperly accessed and obtained by the unauthorized parties. At that time, however, Defendants were fully aware not only that

⁴² *Id.* (emphases added).

⁴³ *Id.*

patient medical information had been obtained by unauthorized parties, but that such information was being offered for sale on the internet as early as November 2015.⁴⁴ Moreover, 21st Century's notification concealed the fact that—due to 21st Century's inadequate and insufficient data security and information retention policies and practices—Defendants never adequately investigated or attempted to ascertain which of their patients had medical information accessed and obtained by unauthorized parties, or offered for sale on the internet.

123. In this regard, the notification letter that 21st Century ultimately mailed to Plaintiffs and Class members failed to provide concrete information about the Data Breach and incompletely described what PII/PHI was in fact exposed, how it was exposed, and what changes 21st Century was making to prevent further compromises of PII/PHI in the future.

3. 21st Century's Notification Was Confusing To Plaintiffs and Class Members

124. When Plaintiffs and Class members began receiving the notification letters from 21st Century on or about March 12, 2016, some of them did not understand that they had a relationship with 21st Century, because 21st Century operates numerous facilities throughout the country under different trade names. For this reason, some Plaintiffs and Class members believed the notification letters they received from 21st Century to be a scam.

125. Indeed, as of March 18, 2016, it was not obvious to Plaintiffs and Class members looking to confirm the authenticity of the notification letter through 21st Century's website that there had been a Data Breach. While a single line, "A Message to Our Patients

⁴⁴ See *infra*.

Regarding Security Incident" appears in small font on the home page of 21st Century's website, it does not prominently appear at the top or bottom of the screen, and is masked amongst other text and images on the elongated home page.



126. For this reason, many recipients of 21st Century's notification letters discarded the letters and did not take action to obtain the credit monitoring services offered

by 21st Century during the short four-month window that 21st Century allowed Plaintiffs and Class members to sign up for the offered services.

127. Other Data Breach victims who were unfamiliar with the name “21st Century Oncology” were left to play detective to ascertain which physicians they had seen, if any, who were associated with 21st Century.

4. Industry Insiders Confirm That 21st Century’s Data Breach Notification Was Insufficient and Inadequate

128. Ted Harrington, executive partner with Independent Security Evaluators, a security assessment and consulting firm, expressed the opinion that 21st Century’s notification was inadequate and misleading:

21st Century Oncology’s response really misses the mark. They note in their statement that no medical records were lost. But patient names, Social Security numbers and other data were. These are some of the most important aspects of the medical record.⁴⁵

129. The U.S. Department of Health & Human Services (“HHS”) is responsible for enforcing rules promulgated under HIPAA. Senior HHS advisor Rachel Seeger has interpreted HIPAA as protecting names and Social Security Numbers:

The personally identifiable information that HIPAA-covered health plans maintain on enrollees and members—including names and Social Security Numbers—is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed.⁴⁶

130. For the foregoing reasons, 21st Century’s delayed and inadequate notification of the Data Breach resulted in additional damage and created additional hardships for

⁴⁵ Paul Benjou, *Negligence is the Cancer of CyberCrime* (Mar. 2016), <http://myopenkimono.blogspot.com/search?q=negligence+is+the+cancer.html> (last visited Jan. 17, 2017).

⁴⁶ Elizabeth Weise, *Anthem Fined \$1.7 million in 2010 breach* (Feb. 5, 2015), <http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345/> (last visited Jan. 17, 2017).

Plaintiffs and Class members who were already experiencing medical and financial difficulties.

E. 21st Century Acknowledged Its Duty To Keep PII/PHI Private

131. 21st Century routinely requests, records, collects and/or generates protected PHI about its patients that includes, but is not limited to, patient names, Social Security numbers, physicians' names, diagnoses and treatment information, and insurance information.

132. 21st Century has acknowledged since at least its March 26, 2013 Notice of Privacy Practices⁴⁷ that it is required by law to maintain the privacy of Plaintiffs' and Class members' PII/PHI and notify them if their PII/PHI was compromised in compliance with applicable law.

Our Responsibilities

We are required by law to maintain the privacy of your protected health information, to provide you with notice of our legal duties and privacy practices with respect to that protected health information, and to notify any affected individuals following a breach of any unsecured protected health information. We will abide by the terms of the notice currently in effect.

21st Century, however, failed to fulfill these responsibilities.

133. Federal and state laws and regulations, including but not limited to the HIPAA Privacy and Security Rules, the HITECH Act, the Federal Trade Commission Act, 16 C.F.R. Part 681 (Identity Theft Red Flags), Federal Register 45 C.S.F. Parts 160 and 164 (Encryption / Destruction Guidance for PHI), 21 C.F.R. Part 11 (Electronic Records); the Arizona Consumer Fraud Act, the California Customer Records Act, the California Confidentiality of Medical Information Act, the California Consumers Legal Remedies Act,

⁴⁷ 21st Century, *Notice of Privacy Practices* (Mar. 26, 2013), <https://www.21co.com/company/hipaa-notice-of-privacy-practices> (last visited Mar. 18, 2016).

the Florida Deceptive and Unfair Trade Practices Act, the Florida Information Protection Act, the Kentucky Consumer Protection Act, the Massachusetts Consumer Protection Act, the Massachusetts Right to Privacy Statute, the Massachusetts Data Protection Act, the New Jersey Consumer Fraud Act, and the Rhode Island Deceptive Trade Practices Act, provide guidelines on the practices healthcare providers should implement to secure patients' confidential medical information.

134. 21st Century violated its duties under the aforementioned laws and regulations by failing to implement adequate and reasonable policies, processes, training, and safeguards, including data privacy and cybersecurity software and hardware, to protect its patients' confidential PII/PHI.

135. 21st Century violated its duties under the aforementioned laws and regulations by failing to follow best practices in the healthcare security.

136. 21st Century violated its duties under the aforementioned laws and regulations by failing to adequately respond to notification of the breach and remediate the effects of the breach.

137. 21st Century's violations of its duties were directly related to the confidential PII/PHI of more than 2.2 million patients being accessed by unauthorized parties.

1. HIPAA Provides Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

138. As a healthcare provider, 21st Century is subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the

Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, “Privacy and Security Rules”).

139. The Privacy and Security Rules establish a national set of standards for the protection of “individually identifiable health information” that is held or transmitted by a health care provider, which HIPAA refers to as “protected health information.”

140. Pursuant to HIPAA, 21st Century must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.

141. HIPAA imposes general security standards that 21st Century must follow, including:

- (a) Ensuring the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits, 45 C.F.R. § 164.306(a);
- (b) Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information, 45 C.F.R. § 164.306(a);
- (c) Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA, 45 C.F.R. § 164.306(a); and
- (d) Reviewing and modifying the security measures implemented under HIPAA as needed to continue provision of reasonable and appropriate protection of electronic protected health information, 45 C.F.R. § 164.306(e).

142. From a technical standpoint, HIPAA requires 21st Century to, among other things:

- (a) Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, 45 C.F.R. § 164.312(a);
- (b) Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, 45 C.F.R. § 164.312(d); and
- (c) Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, 45 C.F.R. § 164.312(e).

143. The HIPAA Security Rule requires 21st Century to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. 45 CFR 164.316(a). These policies and procedures must be maintained in written form. 45 CFR 164.316(b)(1)(i).

144. The HIPAA Security Rule requires covered entities to maintain a written record of any action, activity, or assessment required to be documented by the HIPAA Security Rule. 45 CFR 164.316(b)(1)(ii).

145. The HIPAA Security Rule requires covered entities to review documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. 45 CFR 164.316(b)(1)(iii).

146. Under the HIPAA Privacy Rule, 21st Century may not use or disclose PHI or confidential medical information except as expressly permitted. 45 CFR 164.502(a).

2. The HITECH Act Provides Additional Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

147. The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub.L. 111-5), promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information.

148. The HITECH Act provides lucrative financial incentives, and the avoidance of penalties, to healthcare entities such as 21st Century for demonstrating the meaningful use, interoperability, and security of electronic health information. Achieving meaningful use requires compliance with objectives, measures and certification and standards criteria. The Electronic Health Records (“EHR”) Incentive Program requires compliance with the objective to protect electronic health information. A Core Measure to determine compliance with the objective is conducting or reviewing a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) (the HIPAA Security Rule) and implementing security updates as necessary and correcting identified security deficiencies as part of its risk management process.

149. Upon information and belief, 21st Century implanted a rushed and substandard EHR infrastructure in order to, in part, obtain millions of dollars in lucrative financial incentives, as well as the avoidance of penalties, despite knowing they were ill-equipped and unprepared to safely store and meaningfully use electronic health records and electronic health information in a secure manner consistent with regulations and industry standards.

3. 21st Century Is Subject To Other Federal and State Laws and Regulations That Provide Guidelines on the Practices It Should Have Implemented To Secure Patients' Protected Health Information

150. Section 5(a) of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, prevents 21st Century from using “unfair or deceptive acts or practices in or affecting commerce.” The FTC has found that inadequate data privacy and cybersecurity practices can constitute unfair or deceptive practices that violate § 5.

151. The state of Florida requires companies to maintain electronic PII/PHI in a certain way. Among other things, Florida law requires 21st Century to (1) take reasonable measures to protect and secure data in electronic form containing PII/PHI; (2) take reasonable measures to dispose or destroy PII/PHI; and (3) provide notice to consumers and consumer reporting agencies when a data security incident occurs that compromises PII/PHI. Fla. Stat. § 501.171.

152. The state of California generally prohibits healthcare providers from disclosing a patient’s confidential medical information without prior authorization. The California Confidentiality of Medical Information Act (“CMIA”) (Cal. Civ. Code § 56.10(a)) states that “a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c).” *See also* Cal. Civ. Code §§ 1798.80, *et seq.*

153. The Commonwealth of Massachusetts requires any “person” that “owns or licenses” “personal information” of a resident of the Commonwealth to (1) protect the security and confidentiality of customer information “consistent with industry standards;” (2)

“protect against unanticipated threats or hazards to the security or integrity of customer information” and (3) “protect against unauthorized access to or use of customer information that may result in substantial harm or inconvenience to any consumer.” *See* 201 Mass. Code Regs. § 17.00, *et seq.*; *see also* Mass. Gen Laws Ch. 93H, § 3(a).

154. The state of Rhode Island requires persons who store, collect, process, maintain, acquire, use, own, or license personal information about a Rhode Island resident to implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization. R.I. Gen. Laws § 11-49.3-2.

155. In addition to their obligations under federal and state laws and regulations, 21st Century owed a common law duty to Plaintiffs and Class members to protect PII/PHI entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

156. 21st Century further owed and breached its duty to Plaintiffs and the Class to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems (*e.g.* 45 CFR §§ 164.308(a), 164.306(d), 164.312, The Office for Civil Rights July 14, 2010 Guidance on Risk Analysis Requirements under the HIPAA Security Rule, etc.).

4. Industry Standards Also Provide Guidelines To Healthcare Providers Regarding Best Practices For Securing Confidential Medical Information

157. 21st Century owed and breached its duties to Plaintiffs and Class members to provide and maintain reasonable security over PII/PHI security consistent with industry standards and requirements including but not limited to Cloud Security Alliance (CSA) Cloud Controls Matrix, CMS Information Security ARS 2010, COBIT 4.1 and 5, Iso/IEX 27001:2005, ISO/IEX 27002:2005; ISO/IEC 27799:2008, U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") Special Publication 800-53, NIST Special Publication 800-61, NIST Special Publication 800-66, and Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations, JCAHO), etc. Likewise, 21st Century owed a duty and breached its duties to Plaintiffs and Class members to design, maintain, and test its security systems and networks to ensure that PII/PHI in 21st Century's possession was adequately secured and protected.

158. The Health Information Trust Alliance ("HITRUST"), which applies healthcare, business, technology and information principles, has established the Common Security Framework ("CSF"), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information.

159. HITRUST's CSF is an information security governance framework that blends the requirements of existing standards and regulations, including federal (HIPAA, HITECH), third party (PCI, COBIT) and government (NIST, FTC).

160. HITRUST's CSF is a widely adopted framework in the United States healthcare industry.

161. ISACA, formerly known as Information Systems Audit and Control Association, is an independent, nonprofit, global association that provides practical guidance, benchmarks and other effective tools for all organizations that use information systems.

162. ISACA's Control Objectives for Information and Related Technology ("COBIT") is a framework created by ISACA for IT management and IT governance.

163. HITRUST and COBIT are two examples of best practices related to healthcare information technology governance systems. They both recommend and require measures that take into account HIPAA, HITECH and additional IT security regulations.

F. 21st Century Was Aware of the Risk of Data Breach and the Value of the PII/PHI With Which It Was Entrusted

1. From 2011 To 2012, 21st Century Experienced a Data Breach Involving Patient PII/PHI

164. 21st Century is no stranger to data breaches. On or about May 15, 2013, federal law enforcement officials informed 21st Century that one of its employees had improperly accessed patient PII/PHI over the course of almost ten months between October 11, 2011 and August 8, 2012 (the "2011-2012 Data Breach"). The 21st Century employee provided patient PII/PHI to a third party who used patient names, Social Security numbers, and dates of birth to file fraudulent claims for tax refunds. As with the recently announced Data Breach, 21st Century failed to detect the 2011-2012 Data Breach.

165. When 21st Century notified the Maryland Attorney General of the 2011-2012 Data Breach on or about July 10, 2013, 21st Century had not yet concluded its own internal investigation into how the employee was able to access this information.

166. Ultimately, 21st Century offered victims affected by the 2011-2012 Data Breach one year of credit monitoring and an assurance that “protecting our patients’ personal information is a priority at 21st Century . . . and we take any potential misuse of our patients’ private health information very seriously.”⁴⁸

167. In the ensuing years, however, 21st Century did not carry through with its assurances and only obtained—and thereby put at risk—far more patient data.

2. The FBI Made a Highly Publicized Warning To Healthcare Companies such as 21st Century about the Increased Risk of Cyber Attacks

168. According to cybersecurity company SANS Institute, healthcare providers and health insurance companies are regular targets of cyber-attacks, and were particularly vulnerable to them by October 2013.⁴⁹

169. In April 2014, the FBI’s cyber division warned healthcare systems that cyber-attacks were likely to further increase after January 2015, when healthcare companies were required to switch from using paper medical records to electronic records. The FBI noted that healthcare companies were more susceptible to cyber-attacks, making future attacks likely.⁵⁰

⁴⁸ 21st Century, *Letter to Office of the Attorney General of Maryland* (Jul. 10, 2013), <https://www.oag.state.md.us/idtheft/Breach%20Notices/2013/itu-230673.pdf> (last visited Mar. 18, 2016).

⁴⁹ SANS Institute, *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon* (Feb. 2014), <http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735> (last visited Mar. 18, 2016).

⁵⁰ Federal Bureau of Investigation, *FBI Cyber Division Private Industry Notification* (Apr. 8, 2014), <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf> (last visited Mar. 18, 2016).

170. The FBI's report was highly publicized in 2014, being reported by such news agencies as Reuters.⁵¹

171. However, 21st Century did not heed these warnings to reasonably and adequately secure this private and highly sensitive PII/PHI, as demonstrated by its failure to learn of the recently disclosed Data Breach until the FBI (again) reported it to 21st Century.

172. As Twistlock's chief strategy officer Chenxi Wang told *ESecurity Planet*:

The fact that many of these breaches are reported by the FBI, rather than discovered by the company that holds the data, speaks to the heart of the problem—many organizations do not have sufficient technical expertise and capabilities in place to protect data and respond in a timely manner in the event of a breach[.]⁵²

G. 21st Century Has a Marked History of Prioritizing Profit Over Patients, Performing Unnecessary Tests on its Patients for at least Seven Years

173. The Data Breach must be viewed in the context of the 21st Century corporate culture in which it arose. Contrary to its stated commitment to provide “compassionate” cancer care to patients,⁵³ 21st Century, through its wholly-owned subsidiaries, has been subjecting patients to a variety of unnecessary medical testing for years.

⁵¹ Finkle, *Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks*, Reuters (Apr. 23, 2014), <http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusividUSBREA3M1Q920140423> (last visited Mar. 18, 2016).

⁵² Jeff Goldman, *21st Century Oncology Notifies 2.2 Million Patients of Data Breach* (Mar. 11, 2016), <http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html> (last visited Jan. 17, 2017).

⁵³ 21st Century Oncology, *Home Page*, <https://www.21co.com> (last visited Mar. 18, 2016).



174. On March 25, 2013—two months before the FBI informed 21st Century of the 2011-2012 Data Breach—a medical assistant filed a whistleblower suit against a 21st Century subsidiary alleging a scheme to subject patients to unnecessary tests in order to fraudulently collect money from federal healthcare programs from 2008 through 2012.⁵⁴

175. In the words of Special Agent in Charge Shimon Richmond of the Department of Health and Human Services Office of Inspector General: “These tests were ordered to increase profits, not improve the health care of patients.”⁵⁵

176. On December 16, 2015—one month after the FBI informed 21st Century of the recently disclosed Data Breach—21st Century filed an SEC Form 8-K that announced that it was settling the whistleblower suit for \$19.75 million.⁵⁶

177. On October 19, 2015—less than a month before the FBI informed 21st Century of the instant Data Breach—a doctor filed a whistleblower suit against a 21st

⁵⁴ *United States, State of Fl., ex rel. Barnes v. Spellberg, 21st Century and Naples Urology Assoc.*, No. 2:13-cv-228-FtM-99DNF (M.D. Fla.).

⁵⁵ Don Browne, *21st Century Oncology Paying \$19 Million Settlement In False Billing Case*, Southwest Florida Online (Dec. 18, 2015), <http://swflorida.blogspot.com/2015/12/21st-century-oncology-paying-19-million.html> (last visited Jan. 13, 2017).

⁵⁶ 21st Century Oncology, SEC Form 8-K (Dec. 16, 2015), <https://www.21co.com/investors/sec-filings> (last visited Mar. 18, 2016).

Century subsidiary alleging a scheme to subject patients to four categories of unnecessary tests in order to fraudulently collect money from federal healthcare programs from 2009 through 2014.⁵⁷

178. In this case, “[t]he company prioritized profit over medical counsel,” said David L. Scher, counsel for the whistleblowing doctor.⁵⁸

179. Jason Mehta, Assistant U.S. Attorney agreed, stating: “When medical decision-making is influenced by significant financial incentives, patients suffer—and, in this case, patients and taxpayers were bilked for a test of questionable validity that the government contends, in some cases, offered no value or meaning to any healthcare practitioners.”⁵⁹

180. On March 9, 2016—days after publicly disclosing the Data Breach—21st Century filed an SEC Form 8-K announcing that it was settling the second whistleblower suit for \$34.7 million.⁶⁰

⁵⁷ *United States ex rel. Ting v. 21st Century Oncology and So. Fl. Radiation Oncology*, No. 3:14-cv-723-Jax-J32JRK (M.D. Fla.).

⁵⁸ Patricia Brooks, *Medicare Fraud Whistleblower Represented By The Employment Law Group Law Firm Wins \$34.7 Million Settlement In Case Against 21st Century Oncology*, PR Newswire (Mar. 8, 2016), <http://www.prnewswire.com/news-releases/medicare-fraud-whistleblower-represented-by-the-employment-law-group-law-firm-wins-347-million-settlement-in-case-against-21st-century-oncology-300232646.html> (last visited Mar. 18, 2016).

⁵⁹ *Id.*

⁶⁰ 21st Century Oncology, SEC Form 8-K (Mar. 9, 2016), <https://www.21co.com/investors/sec-filings> (last visited Mar. 18, 2016).

H. 21st Century's Response To the Data Breach Has Been Inadequate and Is Insufficient To Address the Ongoing Risks and Harms To Plaintiffs and Class Members

1. The Risk of Identity Theft Is a Major Concern To Plaintiffs and Class Members

181. There is a strong likelihood that Plaintiffs and Class members are already or will become victims of identity theft and fraud, given the breadth of PII/PHI about them that has been taken by unauthorized parties.

182. The likelihood of such identity theft and fraud is significantly increased by the fact that Plaintiffs and Class members' PII/PHI has already been offered for sale to identity thieves on the internet, as the FBI informed 21st Century in November 2015.

183. As reported by Javelin Strategy & Research's 2014 Identity Fraud Study:

Data breaches are the greatest risk factor for identity fraud. . . . In 2013, one in three consumers who received notification of a data breach became a victim of fraud.⁶¹

184. Hackers steal such PII/PHI in order to sell it on black market sites to identity thieves,⁶² who attempt to get their money's worth from such information by committing identity theft and fraud.

185. The likelihood or probability that Plaintiffs' and Class members' PII/PHI would be improperly used, sold or otherwise mishandled led 21st Century to offer one year of credit monitoring and identity-theft protection to 2.2 million people in its database after

⁶¹ 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, Javelin Strategy, (Feb. 20, 2013), <https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters> (last visited Mar. 18, 2016).

⁶² Ozzie Fonseca, Following Personal Identifying Information (PII) Down the Black Net Road, Experian (Aug. 11, 2015), <http://www.experian.com/blogs/data-breach/2015/08/11/following-personal-identifying-information-pii-down-the-black-net-road/> (last visited Mar. 18, 2016).

the FBI informed it that patient information was illegally obtained by a third party in October 2015.

186. It costs 21st Century more than a *de minimis* amount to provide these services to the 2.2 million Data Breach victims. Experian currently charges \$15.95 for the offered ProtectMyID service through ProtectMyID's website.⁶³ 21st Century has offered these services to Plaintiffs and Class members because the risk of identity theft to Plaintiffs and Class members cannot be safely disregarded.

2. Compromised Social Security Numbers Have Long-Term Value To Thieves and Long-Term Consequences To Data Breach Victims

187. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."⁶⁴

188. Unfortunately, Plaintiffs and Class members have to wait until they become victims of Social Security number misuse before they can obtain a new one.

189. Even then, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee . . . a fresh start." In fact, "[f]or some victims of identity theft, a new number actually creates new problems."⁶⁵ One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for years unless it is linked to the old compromised number.

⁶³ Experian, *Identity Theft Protection*, <http://www.experian.com/consumer-products/identity-theft-and-credit-protection.html> (last visited Jan 13, 2017).

⁶⁴ Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), <http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html#> (last visited Jan. 17, 2017).

⁶⁵ Social Security Admin., *Identity Theft and Your Social Security Number*, <https://www.ssa.gov/pubs/EN-05-10064.pdf> at pgs. 6-7 (last visited Mar. 18, 2016).

3. Compromised Medical Information Has Even Greater Long-Term Value To Thieves and Consequences for Plaintiffs and Class Members

190. Kunal Rupani, director of product management at Accellion, a private cloud solutions company, told *eSecurity Planet* that it's likely the 21st Century hackers were targeting the Data Breach victims' PHI for its long-term value, stating:

Unlike credit card numbers and other financial data, healthcare information doesn't have an expiration date. As a result, a patient's records can sell on the black market for upwards of fifty times the amount of their credit card number, making hospitals and other healthcare organizations extremely lucrative targets for cybercriminals.⁶⁶

191. PHI—like the type disclosed in the breach—is particularly valuable for cybercriminals. According to SecureWorks (a division of Dell Inc.), “[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market (\$50, on average) than a U.S.-based credit card and personal identity with social security number combined.”⁶⁷ The reason is that thieves “[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market.”⁶⁸

192. Similarly, the FBI Cyber Division, in a April 8, 2014 Private Industry Notification, advised:

Cyber criminals are selling [medical] information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.⁶⁹

⁶⁶ See *supra*, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach.

⁶⁷ What's the Market Value of a Healthcare Record, Dell SecureWorks (Dec. 13, 2012), <https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record> (last visited Jan. 13, 2017).

⁶⁸ *Id.*

⁶⁹ FBI Cyber Division Private Industry Notification, *supra* note 50.

4. Thieves Will Likely Use Plaintiffs' and Class Members' PII/PHI To Hurt Them Far Longer Than One Year

193. Once hackers have such PHI, "they can use it to procure prescription drugs or expensive medical equipment or simply to commit financial fraud—often for months or years before anyone notices."⁷⁰

194. While identity thieves historically sought short-term profit from hacked credit card numbers, hackers today are targeting non-financial information so they can "continue to monetize victims' identities over a longer period of time."⁷¹ As observed by Gemalto vice president and CTO for data protection Jason Hart,

In 2014, consumers may have been concerned about having their credit card numbers stolen, but there are built-in protections to limit the financial risks . . . However, in 2015 criminals shifted to attacks on personal information and identity theft, which are much harder to remediate once they are stolen. ⁷²

195. This truth is notably acknowledged in the ProtectMyID attachment to 21st Century's notification letter to Plaintiffs and Class members, which states that "[i]t is recognized that identity theft can happen months and even years after a data breach."⁷³

5. The Consequences To Victims of Medical Identity Theft Can Be Time Consuming, Financially Devastating, and Even Life Threatening

196. Once use of compromised non-financial PII/PHI is detected, the personal and economic consequences to the data breach victims can be overwhelming. As reported by CreditCards.com:

⁷⁰ Cathleen McCarthy, CreditCards, *How to Spot and Prevent Medical Identity Theft* (Aug. 19, 2014) <http://www.creditcards.com/credit-card-news/spot-prevent-medical-identity-theft-1282.php> (last visited Jan. 13, 2017).

⁷¹ *Id.*

⁷² See *supra*, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach.

⁷³ See *supra*, NH Notification Letter.

The Ponemon Institute found that 36 percent of medical ID theft victims pay to resolve the issue, and their out-of-pocket costs average nearly \$19,000. Even if you don't end up paying out of pocket, such usage can wreak havoc on both medical and credit records, and clearing that up is a time-consuming headache. That's because medical records are scattered. Unlike personal financial information, which is consolidated and protected by credit bureaus, bits of your medical records end up in every doctor's office and hospital you check into, every pharmacy that fills a prescription and every facility that processes payments for those transactions.⁷⁴

197. Research by Ponemon confirms that medical identity theft is costly and complex to resolve, and therefore it is critical for healthcare providers to take additional steps to assist victims resolve the consequences of the theft and prevent future fraud. In a 2014 study, Ponemon found that sixty-five percent (65%) of victims of medical identity theft in the study had to pay an average of \$13,500.00 to resolve the resultant crimes⁷⁵, and only ten percent (10%) of those in the study reported having achieved complete satisfaction in concluding the incident.

198. The average time spent by those respondents who successfully resolved their situation was more than 200 hours, working with their insurer or healthcare provider to make sure their personal medical credentials were secure and verifying the accuracy of their personal health information, medical invoices and claims and electronic health records. Indeed, fifty-nine percent (59%) of the respondents reported that their information was used to obtain healthcare services or treatments, and fifty-six percent (56%) reported that their information was used to obtain prescription pharmaceuticals or medical equipment. Forty-five percent (45%) of respondents said that the medical identity theft incident had a negative

⁷⁴ *Id.*

⁷⁵ Jaclyn Fitzgerald, *Ponemon Institute Study Reveals 21.7% Rise in Medical Identity Theft*, HC Pro (Mar. 2, 2015), <http://www.hipro.com/HIM-313785-865/Ponemon-Institute-study-reveals-217-rise-in-medical-identity-theft.html> (last visited Jan. 10, 2017).

impact on their reputation, primarily because of embarrassment due to the disclosure of sensitive personal health conditions (89% of the respondents), thirty-five percent (35%) said the person committing the fraud depleted their insurance benefits resulting in denial of valid insurance claims, and thirty-one percent (31%) said they lost their health insurance entirely as a result of the medical identity theft. Twenty-nine percent (29%) of the respondents reported that they had to make out-of-pocket payments to their health plan or insurer to restore coverage.

199. Additionally, the study found that almost one-half of medical identity theft victims lose their healthcare coverage as a result of the identity theft, almost one-third have their insurance premiums rise, and forty percent (40%) were never able to resolve their identity theft.

200. The injuries suffered and likely to be suffered by Plaintiffs and Class members are and will be a direct and proximate result of the Data Breach, including:

- (a) theft of their personal and financial information;
- (b) loss or delay of tax refunds as a result of fraudulently filed tax returns;
- (c) costs associated with the detection and prevention of identity theft and unauthorized use of their PII/PHI and financial, business, banking, and other accounts;
- (d) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling credit cards, purchasing credit monitoring and identity theft protection

services (beyond the one-year offered by 21st Century), the imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, including phishing emails and phone scams;

(e) the imminent and certain impending injury flowing from fraud and identity theft posed by their PII/PHI being placed in the hands of hackers;

(f) damages to and diminution in value of their PII/PHI entrusted to 21st Century for the sole purpose of obtaining healthcare services from 21st Century;

(g) money paid to 21st Century for healthcare services during the period of the Data Breach because Plaintiffs and Class members would not have obtained healthcare services from 21st Century had it disclosed that it lacked adequate systems and procedures to reasonably safeguard patients' PII/PHI;

(h) overpayments to 21st Century for healthcare services purchased, in that a portion of the amount paid by Plaintiffs and Class members to 21st Century was for the costs for 21st Century to take reasonable and adequate security measures to protect the Plaintiffs and Class members' PII/PHI of, which 21st Century failed to do; and

(i) personal, professional, or financial harms caused as a result of having their PII/PHI exposed.

201. 21 Century and their agents have received numerous complaints of identity theft from Class members who allege their information has been used fraudulently and without their permission.

202. Furthermore, the Office of Inspector General of the U.S. Department of Health & Human Services has cautioned that the consequences to data breach victims can even be life-threatening:

The damage can be life-threatening to you if the wrong information ends up in your personal medical records.⁷⁶

For instance, if incorrect medical information such as blood type or allergies becomes commingled in a data breach victim's medical records, that misinformation can be deadly if that individual becomes unconscious and needs an emergency transfusion or injection.⁷⁷

6. Many of the Affected Patients Comprise a Vulnerable Population

203. Undergoing treatment for cancer often demands significant amounts of time and energy, and can cause painful side effects. Many cancer patients are unable to monitor their financial accounts and credit reports with the same diligence as healthy individuals. The nature of their diagnosis and treatment renders cancer patients, as a group, more vulnerable to financial fraud and identity theft than healthy individuals.

204. In this regard, James Chappell, Digital Shadows' CTO and co-founder, expressed surprise at 21st Century's failure to protect the PII/PHI of its patients, particularly given their known life circumstances, stating:

The circumstances in these patients' lives were already pretty tough ... I'm surprised 21st Century Oncology weren't better stewards of their patients' data given their circumstances.⁷⁸

⁷⁶ Office of Inspector General, *Medical ID Theft/Fraud Information*, <http://oig.hhs.gov/fraud/medical-id-theft/> (last visited Jan. 13, 2017).

⁷⁷ See *supra*, *How to Spot and Prevent Medical Identity Theft*.

⁷⁸ Tom Spring, *Cancer Clinic Warns 2.2 Million Patients of Records Breach* (Mar. 8, 2016), <https://threatpost.com/cancer-clinic-warns-2-2-million-patients-of-records-breach/116668/> (last visited Mar. 18, 2016).

205. Further, cancer disproportionately affects the elderly. Senior citizens are targeted for financial fraud and identity theft at higher rates than non-senior citizens. Identity theft and financial exploitation are among the most commonly reported forms of fraud perpetrated against the elderly.

7. The Remedy Offered By 21st Century Is Inadequate, and Requires Plaintiffs and Class Members To Expend Time on an Ongoing Basis To Contain their Compromised PII/PHI

206. 21st Century previously offered Plaintiffs and Class members twelve months of credit monitoring and identity theft insurance with ProtectMyID, an Experian product. However, this now unavailable remedy does not fully protect Plaintiffs and Class members against the risk of identity theft and fraud. Further, the twelve-month coverage period provided is insufficient to protect Plaintiffs and Class members as it is far shorter than the period that they are likely to become victims of identity theft and fraud.

207. 21st Century sent out letters on March 4, 2016 to Plaintiffs and Class members offering them twelve months of credit monitoring. However, Defendants provided only a very short window of time in which to accept this offer. Plaintiffs and Class members were given only until July 7, 2016—fewer than four months—to receive the letter, learn their options, and decide whether to accept the monitoring. Plaintiffs and Class members who tried enroll in the membership after that date were denied enrollment. This unrealistic deadline posed a problem for Plaintiffs and Class members who initially believed the letter itself was a scam; who did not receive their letter immediately to their current address; who were undergoing treatment and were not able to respond in the short time window; and/or for

those who were still researching their options. Here again, 21st Century placed its financial position before the well-being of its patients.

208. In any event, the previously offered credit monitoring and identity theft insurance cannot fully protect Plaintiffs and Class members against identity theft or fraud. In this regard, credit monitoring is reactionary and only detects activity *after* identity thieves use compromised PII/PHI to attempt to fraudulently open lines of credit. Similarly, identity theft insurance only reimburses losses *after* they have occurred.

209. Accordingly, 21st Century recommended that Plaintiffs and Class members monitor their explanation of benefits statements to detect and resolve unauthorized charges without its help. The notification letter sent by 21st Century to Plaintiffs and Class members stated:

We also recommend that you regularly review the explanation of benefits that you receive from your health insurer. If you see services that you did not receive, please contact your insurer immediately.⁷⁹

210. Further, among the recommendations in the ProtectMyID attachment to 21st Century's Data Breach notification letter to Plaintiffs and Class members was that Data Breach victims take the following steps on their own: (a) "reviewing your credit card, bank, and other financial statements for any unauthorized activity;" (b) obtaining "a copy of your credit report . . . directly from each of the three nationwide credit reporting agencies;" and (c) contacting "the Federal Trade Commission and/or the Office of the Attorney General in your

⁷⁹ See *supra*, NH Notification Letter (emphases added).

home state” for those who believe that they have become “a victim of identity theft or have reason to believe [their] personal information has been misused.”⁸⁰

211. These tasks are significant burdens to ask of anyone who entrusted PII/PHI to another, and it is particularly reprehensible for 21st Century to shift its responsibility to its oncology patients and their loved ones.

212. In sum, the twelve months of credit monitoring and identity theft insurance offered by 21st Century does not in itself adequately protect Plaintiffs and Class members from a lifetime of identity theft risk and does nothing to reimburse Plaintiffs and Class members for the injuries they have already suffered.

VI. CLASS ACTION ALLEGATIONS

213. Plaintiffs bring claims pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Nationwide Class and Statewide Subclasses, as defined below.

A. Nationwide Class

214. Plaintiffs bring their negligence, negligence per se, gross negligence, negligent misrepresentation, breach of express contracts, breach of implied contracts, breach of implied duty of good faith and fair dealing, breach of fiduciary duty, unjust enrichment, invasion of privacy, and declaratory judgment claims (Counts I-X) on behalf of a proposed nationwide class (“Nationwide Class”), defined as follows:

All natural persons in the United States whose PII/PHI was compromised as a result of the Data Breach.

⁸⁰ *Id.*

B. Statewide Subclasses

215. Plaintiffs bring their state consumer protection, data protection, and/or right to privacy statute claims (Counts I-XI) on behalf of separate statewide subclasses for each of the following states:

- a. Arizona
- b. California
- c. Florida
- d. Kentucky
- e. Massachusetts
- f. New Jersey
- g. Rhode Island

Each proposed statewide subclass (“Statewide Subclass”) is defined as follows:

All natural persons who are citizens of [STATE] whose PII/PHI was compromised as a result of the Data Breach.

216. Plaintiffs also bring their negligence, negligence per se, gross negligence, negligent misrepresentation, breach of express contracts, breach of implied contracts, breach of implied duty of good faith and fair dealing, breach of fiduciary duty, unjust enrichment, invasion of privacy, and declaratory judgment claims (Counts I-XI) separately on behalf of each of the Statewide Subclasses, in the alternative to bringing those claims on behalf of the Nationwide Class.

217. Except where otherwise noted, “Class members” shall refer to members of the Nationwide Class and each of the Statewide Subclasses.

218. Excluded from the Nationwide Class and the Statewide Subclasses are Defendants and their current employees, as well as the Court and its personnel presiding over this action.

219. **Numerosity.** The proposed Class is sufficiently numerous, as 2.2 million Data Breach victims had their PII/PHI compromised, and they are dispersed throughout the United States, making joinder of all members impracticable. Class members can be readily identified and ascertained through the records maintained by 21st Century.

220. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members, including:

- a. Whether 21st Century had a legal duty to use reasonable security measures to protect Class members' PII/PHI;
- b. Whether 21st Century timely, accurately, and adequately informed Class members that their PII/PHI had been compromised;
- c. Whether 21st Century breached its legal duty by failing to protect Class members' PII/PHI;
- d. Whether 21st Century acted reasonably in securing Class members' PII/PHI;
- e. Whether Class members are entitled to actual damages and/or statutory damages; and
- f. Whether Class members are entitled to injunctive relief.

221. **Typicality.** Plaintiffs' claims are typical of the claims of members of the proposed Class because, among other things, Plaintiffs and Class members sustained similar

injuries as a result of 21st Century's uniform wrongful conduct and their legal claims all arise from the same conduct by 21st Century.

222. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Plaintiffs' interests do not conflict with Class members' interests and they have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class.

223. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing 21st Century's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

224. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). 21st Century has acted or refused to act on grounds that apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

225. **Rule 23(c)(4).** This action also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims of Class members are composed of particular issues that are common to all Class members and capable of class wide resolution that will significantly advance the litigation.

VII. CAUSES OF ACTION

COUNT I NEGLIGENCE

(On Behalf of the Nationwide Class and Each of the Statewide Subclasses)

226. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

227. 21st Century owed a duty to Plaintiffs and Class members, arising from the sensitivity of the information, the expectation that information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing 21st Century's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' information was adequately secured from unauthorized access.

228. 21st Century's Notice of Privacy Practices acknowledged 21st Century's duty to adequately protect Plaintiffs' and Class members' PII/PHI.

229. 21st Century owed a duty to Plaintiffs and Class members to implement administrative, physical and technical safeguards, such as intrusion detection processes that

detect data breaches in a timely manner, to protect and secure Plaintiffs' and Class members' PII/PHI.

230. 21st Century also had a duty to only maintain PII/PHI that was needed to serve patient needs.

231. 21st Century owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class members' PII/PHI.

232. 21st Century also had independent duties under Plaintiffs' and Class members' state laws that required 21st Century to reasonably safeguard Plaintiffs' and Class members' PII/PHI, and promptly notify them about the Data Breach.

233. 21st Century had a special relationship with Plaintiffs and Class members as a result of being entrusted with their PII/PHI, which provided an independent duty of care. Plaintiffs' and Class members' willingness to entrust 21st Century with their PII/PHI was predicated on the understanding that 21st Century would take adequate security precautions. Moreover, 21st Century was capable of protecting its networks and systems, and the PII/PHI it stored on them, from unauthorized access.

234. 21st Century breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiffs' and Class members' PII/PHI, including administrative, physical and technical safeguards; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiffs' and Class members' PII/PHI; and (d) failing to provide adequate and timely notice of the Data Breach to Plaintiffs and Class members.

235. But for 21st Century's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiffs' and Class members' PII/PHI, Plaintiffs' and Class members' PII/PHI would not have been accessed by unauthorized parties.

236. Plaintiffs and Class members were foreseeable victims of 21st Century's inadequate data security practices. 21st Century knew or should have known that a breach of its data security systems would cause damage to Plaintiffs and Class members.

237. It was reasonably foreseeable, particularly given legal mandates governing health data protection and the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiffs' and Class members' PII/PHI would result in unauthorized access to 21st Century's networks, databases, and computers that stored or contained Plaintiffs' and Class members' PII/PHI.

238. As a result of 21st Century's negligent failure to prevent the Data Breach, Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiffs' and Class members' PII/PHI has also diminished the value of the PII/PHI.

239. The harm to Plaintiffs and Class members was a proximate, reasonably foreseeable result of 21st Century's breaches of its aforementioned duties.

240. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE
(On Behalf of the Nationwide Class and Each of the Statewide Subclasses Excluding California)

241. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

242. Under the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, 21st Century had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs’ and Class members’ PII/PHI.

243. Under HIPAA, 42 C.F.R. 160, *et seq.*, 21st Century had a duty to implement reasonable safeguards to protect Plaintiffs’ and Class members’ PII/PHI.

244. In addition, under state data security statutes (*see, e.g.*, Cal. Civ. Code § 56, *et seq.*; Cal. Civ. Code § 1798.81.5; Fla. Stat. § 501.171; Fla. Stat. § 456.057; Mass. Gen. Laws Ch. 93H, § 3(a); R.I. Gen. Laws § 11-49.3-2) 21st Century had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs’ and Class members’ PII/PHI.

245. 21st Century breached its duties to Plaintiffs and Class members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 C.F.R. 160, *et seq.*), and the state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs’ and Class members’ PII/PHI.

246. Plaintiffs and Class members were foreseeable victims of 21st Century’s violations of the FTCA, HIPAA, and state data security statutes. 21st Century knew or

should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class members' PII/PHI would cause damage to Plaintiffs and Class members.

247. 21st Century's failure to comply with the applicable laws and regulations constitutes negligence *per se*.

248. But for 21st Century's violation of the applicable laws and regulations, Plaintiffs' and Class members' PII/PHI would not have been accessed by unauthorized parties.

249. As a result of 21st Century's failure to comply with applicable laws and regulations, Plaintiffs and Class members suffered injury, which includes, but is not limited to, the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class members' PII/PHI has also diminished the value of the PII/PHI.

250. The harm to Plaintiffs and the Class members was a proximate, reasonably foreseeable result of 21st Century's breaches of the applicable laws and regulations.

251. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

**COUNT III
GROSS NEGLIGENCE**

(On Behalf of the Nationwide Class and Each of the Statewide Subclasses)

252. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

253. Plaintiffs and Class members entrusted 21st Century with highly-sensitive and inherently personal private data subject to confidentiality laws and physician-patient privileges.

254. In requiring, obtaining and storing Plaintiffs' and Class members' PII/PHI, 21st Century owed a duty of reasonable care in safeguarding the PII/PHI.

255. 21st Century's networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class members' PII/PHI were secured from unauthorized access.

256. 21st Century Oncology's networks, systems, protocols, policies, procedures and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class members' private data and the known vulnerabilities of 21st Century's systems.

257. 21st Century did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

258. Upon learning of the Data Breach, 21st Century should have immediately disclosed the Data Breach to Plaintiffs and Class members, credit reporting agencies, the Internal Revenue Service, financial institutions and all other third parties with a right to know

and the ability to mitigate harm to Plaintiffs and Class members as a result of the Data Breach.

259. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class members' PII/PHI were secured from unauthorized access, 21st Century ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

260. 21st Century's behavior establishes facts evidencing a reckless disregard for Plaintiffs' and Class members' rights.

261. 21st Century, therefore, was grossly negligent.

262. 21st Century's negligence also constitutes negligence per se.

263. The negligence is directly linked to injuries.

264. As a result of 21st Century's reckless disregard for Plaintiffs' and Class members' rights by failing to failing to secure their PII/PHI despite knowing its networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested, Plaintiffs and Class members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The

Unauthorized acquisition of Plaintiffs' and Class members' PII/PHI has also diminished the value of their PII/PHI.

265. The harm to Plaintiffs and the Class members was a proximate, reasonably foreseeable result of 21st Century's breaches of the applicable laws and regulations.

266. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT IV
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class and Each of the Statewide Subclasses)

267. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

268. 21st Century negligently and recklessly misrepresented material facts pertaining to the provision of healthcare services to Plaintiffs and Class Members by representing they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class members' PII/PHI from unauthorized disclosure, release, data breaches, and theft.

269. 21st Century negligently and recklessly misrepresented material facts pertaining to the provision of healthcare services to Plaintiffs and Class members by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiffs' and Class members' PII/PHI.

270. Prior to making these representations, 21st Century knew its networks, systems, protocols, policies, procedures and practices, as described above, were not

adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class members' PII/PHI were secured from unauthorized access

271. In reliance upon these representations, Plaintiffs and Class members engaged and paid for 21st Century to provide healthcare services to Plaintiffs and Class members.

272. Had Plaintiffs and Class members, as reasonable persons, known of 21st Century's inadequate data privacy and security practices, or that 21st Century was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiffs' and Class members' PII/PHI, they would not have engaged 21st Century to provide, nor paid for, healthcare services from 21st Century, and would not have entrusted their PII/PHI to 21st Century.

273. As a direct and proximate consequence of 21st Century's negligent misrepresentations, Plaintiffs and Class members have suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class members' PII/PHI has also diminished the value of the PII/PHI.

274. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT V
BREACH OF EXPRESS CONTRACTS
(On Behalf of the Nationwide Class and Statewide Subclasses)

275. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

276. Plaintiffs and members of the Class, additionally and alternatively, allege that they entered into valid and enforceable express contracts, or were third party beneficiaries of valid and enforceable express contracts, with 21st Century.

277. Under these express contracts, 21st Century and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and members of the Class agreed to pay money for these services.

278. Both the provision of healthcare and the protection of Plaintiffs' and Class members' PII/PHI were material aspects of these contracts.

279. At all relevant times, 21st Century expressly represented that it is "required by law" to provide Plaintiffs and Class members with notice of 21st Century's "legal duties and privacy practices with respect to that health information." 21st Century's Notice of Privacy Practices that was published on 21st Century's website at all times relevant hereto, for example, expressly represented that 21st Century would "abide by the terms of the notice currently in effect," which included maintaining "the privacy of your protected health information" as required by law.⁸¹ 21st Century also expressly represented in the Notice of

⁸¹ See *supra*, 21st Century, *Notice of Privacy Practices*.

Privacy Practices that it would notify any affected individuals following a breach of any unsecured protected health information.⁸²

280. 21st Century's express representations, including, but not limited to, express representations found in 21st Century's Notice of Privacy Practices, formed an express contract requiring 21st Century to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' PII/PHI.

281. Alternatively, the express contracts included implied terms requiring 21st Century to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' PII/PHI, including in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

282. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiffs and Class members, healthcare that does not adhere to industry-standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class members would not have entered into these contracts with 21st Century and/or its affiliated healthcare providers as a direct or third party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

283. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PII/PHI to 21st Century and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

⁸² *Id.*

284. 21st Century materially breached the terms of these express contracts, including but not limited to the terms stated in the relevant Notice of Privacy Practices. 21st Century did not “maintain the privacy” of Plaintiffs’ and Class members’ PII/PHI as “required by law” as evidenced by its notifications of the Data Breach to Plaintiffs and 2.2 million Class members. Specifically, 21st Century did not comply with HIPAA, federal, state and local laws, or industry standards, or otherwise protect Plaintiffs’ and the Class members’ PII/PHI, as set forth above. Further, on information and belief, 21st Century has not yet provided Data Breach notifications to some affected Class members who may already be victims of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud associated with PII/PHI that they provided to 21st Century. These Class members are as yet unaware of the potential source for the compromise of their PII/PHI.

285. The Data Breach was a reasonably foreseeable consequence of 21st Century’s actions in breach of these contracts.

286. As a result of 21st Century’s failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value of the secure healthcare they paid for and the healthcare they received.

287. Had 21st Century disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class members, nor

any reasonable person would have purchased healthcare from 21st Century and/or its affiliated healthcare providers.

288. As a result of 21st Century's breach, Plaintiffs and members of the Class suffered actual damages resulting from the theft of their PII/PHI, as well as the loss of control of their PII/PHI, and remain in imminent risk of suffering additional damages in the future.

289. Also as a result of 21st Century's breach, Plaintiffs and the Class members have suffered actual damages resulting from their attempt to mitigate the effects of the breach of contract and subsequent Data Breach, including but not limited to, purchasing credit monitoring and taking other steps to protect themselves from the loss of their PII/PHI.

290. Accordingly, Plaintiffs and the other members of the Class have been injured as a result of 21st Century's breach of contracts and are entitled to damages and/or restitution in an amount to be determined at trial.

COUNT VI
BREACH OF IMPLIED CONTRACTS
(On Behalf of the Nationwide Class and Statewide Subclasses)

291. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

292. Plaintiffs and Class members were required to provide their PII/PHI to obtain healthcare from affiliated providers of 21st Century, and/or 21st Century. Plaintiffs and Class members entrusted their PII/PHI to 21st Century and/or its affiliated healthcare providers in order to obtain healthcare from them.

293. By providing their PII/PHI, and upon 21st Century's acceptance of such information, Plaintiffs and Class members on one hand, and 21st Century on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning health care, whereby, 21st Century was obligated to take reasonable steps to secure and safeguard that information.

294. 21st Century had an implied duty of good faith to ensure that the PII/PHI of Plaintiffs and Class members in its possession was only used in accordance with their contractual obligations.

295. 21st Century was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class members' PII/PHI and to comply with industry standards and state laws and regulations for the security of this information, and 21st Century Oncology expressly assented to these terms in its Notice of Privacy Practices as alleged above.

296. Under these implied contracts for data security, 21st Century was further obligated to provide Plaintiffs and all Class members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII/PHI.

297. Plaintiff and Class members performed all conditions, covenants, obligations, and promises owed to 21st Century, including paying for the medical care associated with 21st Century and/or providing the PII/PHI required to 21st Century and/or its affiliate providers.

298. 21st Century breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class members' PII/PHI, resulting in

the Data Breach. 21st Century unreasonably interfered with the contract benefits owed to Plaintiffs and Class members.

299. Further, on information and belief, 21st Century has not yet provided Data Breach notifications to some affected Class members who may already be victims of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud associated with the PII/PHI that they provided to 21st Century. These Class members are unaware of the potential source for the compromise of their PII/PHI.

300. The Data Breach was a reasonably foreseeable consequence of 21st Century's actions in breach of these contracts.

301. As a result of 21st Century's conduct, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare that was of a diminished value to the secure healthcare they paid for. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value of the secure healthcare they paid for and the healthcare they received.

302. Neither Plaintiffs, Class members, nor any reasonable person would have provided their PII/PHI to 21st Century and/or its affiliate providers had 21st Century disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

303. As a result of 21st Century's breach, Plaintiffs and members of the Class have suffered actual damages resulting from theft of their PII/PHI, as well as the loss of control of their PII/PHI, and remain in imminent risk of suffering additional damages in the future.

304. Also as a result of 21st Century's breach, Plaintiffs and the Class members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including but not limited to purchasing credit monitoring and taking other steps to protect themselves from the loss of their PII/PHI. As a result, Plaintiffs and the Class members have suffered actual identity theft and the ability to control their PII/PHI.

305. Accordingly, Plaintiffs and Class members have been injured as a result of 21st Century's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT VII
BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING
(On Behalf of the Nationwide Class and Statewide Subclasses)

306. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

307. Plaintiffs and Class members entered into and/or were the beneficiaries of contracts with Defendants and their affiliates, as alleged above.

308. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendants and their affiliates would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the

confidentiality of Plaintiffs' and Class members' PII/PHI and to comply with industry standards and federal and state laws and regulations for the security of this information.

309. Special relationships exist between Defendants and their affiliates and Plaintiffs and Class members. Defendants and their affiliates entered into special relationships with Plaintiffs and Class members who entrusted their confidential PII/PHI to Defendants and their affiliates and paid for medical services with Defendants.

310. Defendants and their affiliates promised and were obligated to protect the confidentiality of Plaintiffs' and Class Members' PII/PHI from disclosure to unauthorized parties. Defendants breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII/PHI, which resulted in the Data Breach. Defendants unreasonably interfered with the contract benefits owed to Plaintiffs and Class members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the PII/PHI of Plaintiffs and the Class in Defendants' possession.

311. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants, including paying Defendants and their affiliates for medical services and providing them the confidential PII/PHI required by the contracts.

312. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class members did not receive the full benefit of their bargain—medical services with reasonable data privacy—and instead received medical services that were less valuable than what they paid for and less valuable than their reasonable

expectations under the contracts. Plaintiffs and Class members have suffered actual damages in an amount equal to the difference in the value between medical care with reasonable data privacy that Plaintiffs and Class members paid for, and the medical care they received without reasonable data privacy.

313. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class members have suffered actual damages resulting from the theft of their PII/PHI and remain at imminent risk of suffering additional damages in the future.

314. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach, including but not limited to purchasing credit monitoring services or taking other steps to protect themselves from the loss of their PII/PHI.

315. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their conduct.

COUNT VIII
BREACH OF FIDUCIARY DUTY
(On Behalf of the Nationwide Class and Statewide Subclasses)

316. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

317. Defendants owed a fiduciary duty to Plaintiffs and the Class as guardians of their PII/PHI to (a) protect the PII/PHI belonging to Plaintiffs and members of the Class; and (b) timely notify them of the Data Breach.

318. Defendants breached their fiduciary duty to Plaintiffs and the Class by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) failing to take adequate actions to prevent disclosure of Plaintiffs' and Class members' PII/PHI to unauthorized parties in a manner that is highly offensive to a reasonable person; (c) failing to take adequate actions to prevent disclosure of Plaintiffs' and Class members' PII/PHI to unauthorized parties without the informed and clear consent of Plaintiffs and the Class; and (d) notifying Plaintiffs and the Class of the Data Breach five months after it had occurred and four months after Defendants had knowledge of the Data Breach..

319. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered an injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their conduct.

COUNT IX
UNJUST ENRICHMENT
(Alternative To Breach of Contract Claim)
(On Behalf of the Nationwide Class and Statewide Subclasses)

320. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

321. Plaintiffs and Class members conferred a monetary benefit on Defendants in the form of monetary payments—directly or indirectly—for medical services received.

322. Defendants collected, maintained, and stored the PII/PHI of Plaintiffs and Class members and, as such, Defendants had knowledge of the monetary benefits conferred by Plaintiffs and Class members.

323. The money that Plaintiffs and Class members paid to Defendants should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' PII/PHI. Defendants failed to implement—or adequately implement—adequate data security practices, procedures, and programs to secure sensitive PII/PHI, as evidenced by the Data Breach.

324. As a result of Defendants' failure to implement data security practices, procedures, and programs to secure sensitive PII/PHI, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in the value between medical care with reasonable data privacy that Plaintiffs and Class members paid for, and the medical care they received without reasonable data privacy.

325. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' PII/PHI and that Plaintiffs and Class members paid for.

326. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by

Defendants. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendants traceable to Plaintiffs and the Class.

COUNT X
INVASION OF PRIVACY
(On Behalf of the Nationwide Class and Statewide Subclasses)

327. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

328. Plaintiffs and Class members reasonably expected that their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

329. Defendants unlawfully invaded the privacy rights of Plaintiffs and the Class by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiffs and the Class.

330. In failing to adequately secure Plaintiffs' and Class members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and Class members.

331. Defendants violated Plaintiffs' and Class members' right to privacy under the common law as well as under state law, including but not limited to the California Constitution, Article I, Section I.

332. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiffs' and Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and the Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

COUNT XI
DECLARATORY JUDGMENT
(On Behalf of the Nationwide Class and Statewide Subclasses)

333. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

334. Plaintiffs and the Class have stated claims against Defendants based on negligence, negligence per se, gross negligence negligent misrepresentation, breach of express contract, breach of implied contracts, breach implied duty of good faith and fair dealing, breach of fiduciary duty, unjust enrichment, invasion of privacy and violations of various state and federal statutes.

335. Defendants failed to fulfill their obligations to provide adequate and reasonable data security measures for the PII/PHI of Plaintiffs and the Class, as evidenced by the Data Breach.

336. As a result of the Data Breach, Defendants' system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII/PHI of Plaintiffs and the Class going forward.

337. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' current obligations to provide data security measures adequate to protect the

PII/PHI of Plaintiffs and the Class. Defendants maintain that their security measures were—and still are—reasonably adequate and denies that they previously had or have any obligation to implement better safeguards to protect the PII/PHI of Plaintiffs and the Class.

338. Plaintiffs seek a declaration that Defendants must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to the PII/PHI of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that Defendants' existing security measures do not comply with their obligations, and that Defendants must implement and maintain reasonable data security measures on behalf of Plaintiffs and the Class to comply with their data security obligations.

COUNT XII
Violations of the Arizona Consumer Fraud Act
Ariz. Rev. Stat. Ann. §§ 44-1521, *et seq.*
(On Behalf of the Arizona Subclass)

339. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

340. The Arizona Consumer Fraud Act prohibits “any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged.”

341. Plaintiff and members of the Arizona Subclass are “persons” as defined by Ariz. Rev. Stat. § 44-1521(6).

342. Pursuant to Ariz. Rev. Stat. §§ 44-1521(5) and (7), Defendants engaged in the sale of “merchandise” in the form of medical services.

343. Defendants engaged in deceptive acts or practices by representing to Plaintiff and the Arizona Subclass that they maintain data security practices and procedures to safeguard Arizona Subclass members' PII/PHI from unauthorized disclosure, release, data breaches, and theft, and that they would comply with relevant federal and state laws pertaining to the privacy and security of PII/PHI. Plaintiff and the Arizona Subclass members were misled by Defendants' misrepresentations and reasonably relied upon them to their detriment. Had Plaintiff and the Arizona Subclass members known about Defendants' substandard data security practices, they would not have provided their PII/PHI to Defendants or they would have taken steps to protect themselves from harm that could result from Defendants' substandard data security practices.

344. Defendants engaged in deceptive acts or practices by omitting, suppressing, and concealing the material fact of the inadequacy of their data security protections for the PII/PHI of Plaintiff and the Arizona Subclass. At the time that Plaintiff and Arizona Subclass members provided Defendants their PII/PHI in exchange for medical services, Defendants failed to disclose to Plaintiff and the Arizona Subclass that Defendants' data security systems failed to meet legal and industry standards to protect their PII/PHI. Had Plaintiff and the Arizona Subclass members known about Defendants' substandard data security practices, they would not have provided their PII/PHI to Defendants or they would have taken steps to protect themselves from harm that could result from Defendants' substandard data security practices.

345. 21st Century knew, or should have known, that its computer systems and data security practices and measures failed to meet legal and industry standards to protect the

PII/PHI of Plaintiff and the Arizona Subclass, were inadequate to safeguard the PII/PHI of Plaintiff and the Arizona Subclass, and that the risk of a data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate data security measures to prevent another breach thereafter. 21st Century's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Arizona Subclass members. Defendants' failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer. Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and members of the Arizona Subclass; and (b) defeat Plaintiff's and the Arizona Subclass members' ordinary, foreseeable and reasonable expectations concerning the adequacy of Defendants' data security.

346. An objective, reasonable person would have been deceived by 21st Century's representations about the security and protection of data in its databases and networks.

347. Defendants intended that Plaintiff and the Arizona Subclass rely on their deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with 21st Century's offering of medical services and incorporating Plaintiff's and the Arizona Subclass members' sensitive information on its computer systems, in violation of the Arizona Consumer Fraud Act.

348. Defendants also engaged in unfair acts and practices, in connection with the sale of medical services by failing to maintain the data security of Plaintiffs' and the Arizona Subclass members' PII/PHI in violation of duties imposed by and public policies reflected in

applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including HIPAA (42 U.S.C. § 1302d, *et seq.*).

349. Defendants' wrongful practices, which occurred in the course of trade or commerce, were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendants that applied to Plaintiff and the Arizona Subclass and were repeated continuously before and after Defendants obtained confidential PII/PHI concerning Plaintiff and Arizona Subclass members, all of whom have been adversely affected by Defendants conduct and the public was and is at risk as a result thereof.

350. 21st Century's acts, omissions, and practices proximately caused Plaintiff and Arizona Subclass members to suffer damages including incurring costs associated with protecting PII/PHI that has been exposed; costs associated with the theft of their identities, such as time and expenses associated with credit monitoring, decrease in credit ratings, financial harm suffered as a result of accounts opened and used without their knowledge or authorization, and time and expense associated with closing accounts opened and used without their knowledge or authorization. Plaintiffs and Arizona Subclass members also suffered damages in that they did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) medical goods and services that they otherwise would not have; and they lost their ability to make informed and reasoned decisions about their medical treatment.

351. As a direct and proximate result of Defendants' unfair and deceptive practices, Plaintiff and members of the Arizona Subclass have suffered injuries to legally protected

interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their PII/PHI, including confidential medical records, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

352. As a direct and proximate cause of these practices, Plaintiff and Arizona Subclass members suffered an ascertainable loss.

353. The above unfair and deceptive trade practices and acts by 21st Century were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Arizona Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

354. As a direct and proximate result of 21st Century's unlawful, unfair, and fraudulent business practices, Plaintiff and members of the Arizona Subclass have suffered injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining 21st Century from their unlawful and unfair practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and Arizona Subclass members. 21st Century will continue to maintain Plaintiff's and Arizona Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and Arizona Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Arizona Subclass members.

355. Plaintiff and Arizona Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Arizona Subclass have an

effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under Ariz. Rev. Stat. § 44-1521.

356. Plaintiff and the Arizona Subclass also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and the Arizona private attorney general doctrine *See Arnold v. Ariz. Dep't of Health Servs.*, 160 Ariz. 593, 609 (1989); *Ariz. Ctr. for Law in the Pub. Interest v. Hassell*, 172 Ariz. 356, 371 (App. 1991).

COUNT XIII
Violations of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq.*
(On Behalf of the California Subclass)

357. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

358. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

359. The CMIA further requires that “[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information.” Cal. Civ. Code § 56.101(b)(1)(A).

360. Plaintiffs and California Subclass members are “patient[s],” “whether or not still living, who received health care services from a provider of health care and to whom medical information pertains” pursuant to § 56.05(k) of the CMIA.

361. 21st Century is a “provider of healthcare” pursuant to § 56.05(m) of the CMIA “who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information.”

362. 21st Century is subject to the requirements and mandates of the CMIA.

363. The PHI of Plaintiffs and California Subclass members compromised in the Data Breach constitutes “medical information” maintained in electronic form pursuant to § 56.05(j) of the CMIA.

364. 21st Century violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the PHI of Plaintiffs and California Subclass members, and failing to protect and preserve the integrity of the PHI of Plaintiffs and California Subclass members.

365. Plaintiffs and California Subclass members did not authorize 21st Century’s disclosure and release of their PHI that occurred in the Data Breach.

366. As a result of the Data Breach, the PHI of Plaintiffs and California Subclass members was compromised when it was acquired and accessed by unauthorized parties.

367. 21st Century violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiffs' and California Subclass members' PHI; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and California Subclass members' PHI; (3) failing to use reasonable authentication procedures to track PHI in case of a security breach; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiffs' and California Subclass members' PHI was kept, all in violation of the CMIA.

368. 21st Century's failure to implement adequate data security measures to protect the PHI of Plaintiffs and California Subclass members was a substantial factor in allowing unauthorized parties to access 21st Century's computer systems and acquire the PHI of Plaintiffs and California Subclass members.

369. As a direct and proximate result of 21st Century's violation of the CMIA, 21st Century allowed the PHI of Plaintiffs and California Subclass members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their PHI, thereby breaching the confidentiality of their PHI. Plaintiffs and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

370. Plaintiffs, individually and on behalf of California Subclass members, seek actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

371. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

COUNT XIV
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of the California Subclass)

372. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

373. California's Unfair Competition Law ("UCL"), California Business & Professions Code § 17200, *et seq.*, provides for relief where a defendant's acts, omissions, and practices are shown to be unlawful, unfair, and fraudulent. 21st Century's acts, omissions, and practices constitute unlawful and unfair business practices in violation of the UCL.

374. 21st Century's acts, omissions, and practices constitute unlawful practices and in violation of the Customer Records Act, the CMIA, HIPAA, California Civil Code §§ 1572, 1573, 1709, 1711, 1798.82, 1798.84; California Business & Professions Code §§ 17200, *et seq.*; California Business & Professions Code 17500, *et seq.*, and California common law because 21st Century failed to take adequate security measures in protecting the confidentiality of Plaintiffs' PII/PHI, 21st Century unreasonably delayed informing Plaintiffs and the California Subclass about the Data Breach, and 21st Century negligently released Plaintiffs' and California Subclass members' PII/PHI that was within its possession and control.

375. 21st Century's acts, omissions, and conduct, including those of Defendant 21st Century Oncology of California, a Medical Corporation, also constitute unlawful practices because they failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977, the Customer Records Act, CMIA, and HIPAA, which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal or medical data utilize reasonable data security measures. 21st Century engaged in conduct that undermines or violates the stated policies underlying the California Customer Records Act and other privacy statutes. For instance, in enacting the Customer Records Act, the California Legislature stated that “[i]dentity theft is costly to the marketplace and to consumers” and that “victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative.” 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). Similarly, the Information Practices Act of 1977 was enacted to protect individuals' data and ensure that entities who solicit or are entrusted with personal data use reasonable security measures.

376. 21st Century's acts, omissions, and conduct also constitute unfair business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiffs and California Subclass members. The gravity of harm resulting from 21st Century's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further 21st Century's legitimate business interests. 21st Century's conduct undermines public policy reflected in statutes such as HIPAA and the CMIA.

377. 21st Century's acts, omissions, and conduct further constitute unfair business acts or practices because Plaintiffs and California Subclass members have been substantially injured by the negligent release of their PII/PHI, which outweighs any countervailing benefits to Plaintiffs and California Subclass members. Plaintiffs and California Subclass members could not have reasonably avoided their substantial injuries because they were required to provide 21st Century with their PII/PHI to receive medical services.

378. 21st Century engaged in fraudulent business acts or practices by representing to Plaintiffs and California Subclass members that they maintain adequate data security practices and procedures to safeguard PII/PHI from unauthorized disclosure, release, data breaches, and theft, and that they would comply with relevant federal and state laws pertaining to the privacy and security of PII/PHI. Plaintiffs and California Subclass members were misled by 21st Century's misrepresentations and reasonably relied upon them to their detriment. Had Plaintiffs and California Subclass members known about 21st Century's substandard data security practices, they would not have provided their PII/PHI to 21st Century or they would have taken steps to protect themselves from harm that could result from 21st Century's substandard data security practices.

379. 21st Century engaged in fraudulent business acts or practices by omitting, suppressing, and concealing the material fact of the inadequacy of the data security protections for the PII/PHI of Plaintiffs and California Subclass members. At the time that Plaintiffs and California Subclass members provided 21st Century their PII/PHI for medical services, 21st Century failed to disclose to Plaintiffs and California Subclass members that 21st Century's computer systems and data security practices and measures failed to meet

legal and industry standards, were inadequate to safeguard their PII/PHI and that the risk of data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate security measures to prevent another breach thereafter. Had Plaintiffs and California Subclass members known about Defendants' substandard data security practices, they would not have provided their PII/PHI to 21st Century or they would have taken steps to protect themselves from harm that could result from 21st Century's substandard data security practices.

380. 21st Century's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and California Subclass members. Defendants' failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer. Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and members of the California Subclass; and (b) defeat Plaintiff's and the California Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of Defendants' data systems.

381. An objective, reasonable person would have been deceived by 21st Century's representations about the security and protection of data in its databases and networks.

382. As a direct and proximate result of 21st Century's unlawful, unfair, and fraudulent business practices, Plaintiffs and members of the California Subclass have suffered injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining 21st Century from their unlawful and unfair practices. 21st Century's conduct caused and continues to cause substantial injury to

Plaintiffs and California Subclass members. 21st Century will continue to maintain Plaintiffs' and California Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiffs and California Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and California Subclass members.

383. Plaintiffs and California Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the California Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under the UCL.

384. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT XV
Violations of the California Customer Records Act
Cal. Civ. Code § 1798.81.5, *et seq.*
(On Behalf of the California Subclass)

385. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

386. Plaintiffs bring this cause of action on behalf of the California Subclass.

387. The California Legislature enacted California Civil Code § 1798.81.5 “to ensure that personal information about California residents is protected.” The statute requires that any business that “owns, licenses, or maintains personal information about a California resident . . . implement and maintain reasonable security procedures and practices

appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” 21st Century is a “business” as defined by California Civil Code § 1798.80(a).

388. Plaintiffs and California Subclass members are each a “customer” pursuant to Civil Code § 1798.80(c) as they each “provide[d] personal information to [Defendants] for the purpose of . . . obtaining a service from [Defendants].”

389. Plaintiffs and California Subclass members are each also an “individual” as defined by Civil Code § 1798.80(d).

390. The PII/PHI compromised in the Data Breach constitutes “personal information” as defined by California Civil Code §§ 1798.80(e) and 1798.81.5(d), which includes “information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, . . . insurance policy number, . . . bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.”

391. As defined by California Civil Code § 1798.82(g), the Data Breach constitutes a “breach of the security of the system” of 21st Century “that compromise[d] the security, confidentiality, or integrity of personal information maintained by [21st Century].”

392. By failing to implement reasonable data security measures appropriate to the nature of the personal information of its current and former patients and customers, 21st Century violated California Civil Code § 1798.81.5.

393. 21st Century further violated California Civil Code § 1798.82 by failing to notify all affected individuals that their PII/PHI had been acquired, or reasonably believed to have been acquired, by unauthorized persons in the Data Breach without unreasonable delay. Instead, 21st Century waited five months after the Data Breach had occurred, and four months after receiving knowledge of the Data Breach, before notifying Plaintiffs and California Subclass members. Timely disclosure of the Data Breach would have allowed Plaintiffs and California Subclass members to take appropriate measures to protect themselves from or ameliorate the damages caused by the Data Breach, including placing security freezes on their credit before any fraudulent accounts could be opened in their names using their Social Security numbers and other PII/PHI, obtaining credit monitoring services, monitoring their PII/PHI and credit reports for fraudulent activity, and contacting government agencies and the local police.

394. As a result of 21st Century's violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass members have sustained and will continue to sustain actual damages as set forth above.

395. Plaintiffs seek all remedies available under California Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

396. Due to 21st Century's violations of California Civil Code §§ 1798.81.5 and 1798.82, Defendants "may be enjoined" under § 1798.84(e) of the same title. Accordingly, Plaintiffs seek an injunction requiring Defendants to formulate, adopt, and implement a data

security plan that prevents unauthorized access to PII/PHI. 21st Century's conduct caused and continues to cause substantial injury to Plaintiffs and California Subclass members. 21st Century will continue to maintain Plaintiffs' and California Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiffs and California Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and California Subclass members.

397. Plaintiffs and California Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the California Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under California Civil Code § 1798.84(e).

COUNT XVI
Violations of the California Consumers Legal Remedies Act (“CLRA”)
Cal. Civ. Code § 1750, *et seq.*
(On Behalf of the California Subclass)

398. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

399. Plaintiffs bring this cause of action on behalf of the California Subclass.

400. The Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.* (the “CLRA”) has adopted a comprehensive statutory scheme prohibiting various deceptive practices in connection with the conduct of a business providing goods, property, or services to consumers primarily for personal, family, or household purposes. The self-declared purposes of the CLRA are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection.

401. Defendants are “persons” within the meaning of California Civil Code § 1761(c), and provided “services” within the meaning of California Civil Code § 1761(b).

402. Plaintiffs and California Subclass members are “consumers” within the meaning of California Civil Code § 1761(d) who engaged in a “transaction” within the meaning of California Civil Code § 1761(e).

403. Section 1770(a)(5) of the CLRA prohibits any entity from “[r]epresenting that goods or services have . . . characteristics, . . . benefits . . . which they do not have” 21st Century represented that their data security practices and procedures were adequate to secure Plaintiffs’ and California Subclass members’ PII/PHI when in fact its data security systems were susceptible to breach, as evidenced by the occurrence of the Data Breach.

404. Section 1770(a)(7) of the CLRA prohibits anyone from “[r]epresenting that goods or services are of a particular standard, quality, or grade, . . . if they are of another.” 21st Century represented that their data security practices and procedures were adequate to secure Plaintiffs’ and California Subclass members’ PII/PHI when in fact its data security systems were susceptible to breach, as evidenced by the occurrence of the Data Breach.

405. 21st Century knew, or should have known, that its computer systems and data security practices and measures failed to meet legal and industry standards, were inadequate to safeguard the PII/PHI of Plaintiffs and California Subclass members and that the risk of data breach or theft was highly likely, including but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate data security measures to prevent another breach thereafter. Had Plaintiffs known about 21st Century’s substandard data security practices, they would not have provided their PII/PHI to 21st

Century or they would have taken steps to protect themselves from harm that could result from 21st Century's substandard data security practices. 21st Century's failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer.

406. An objective, reasonable person would have been deceived by 21st Century's representations about the security and protection of data in its databases and networks.

407. A written pre-suit demand under California Civil Code § 1782(a) is unnecessary and unwarranted because 21st Century has had notice of Plaintiffs' allegations, claims and demands through the filing of numerous underlying actions arising from the Data Breach since March 18, 2016. Any pre-suit notice would not put 21st Century in a better position to evaluate those claims.

408. As a direct and proximate result of 21st Century's violations of the CLRA, Plaintiffs and California Subclass members have suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining 21st Century from their unlawful practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiffs and California Subclass members. 21st Century will continue to maintain Plaintiffs' and California Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiffs and California Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and California Subclass members.

409. Plaintiffs and California Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the California Subclass

have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under CLRA.

410. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT XVII
Violations of the Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. § 501.201, *et seq.*
(On Behalf of the Florida Subclass)

411. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

412. 21st Century's business practices alleged herein constitute unfair and/or deceptive methods, acts, or practices under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.* ("FDUTPA").

413. At all relevant times, Florida Subclass members were "consumers" within the meaning of the FDUTPA, Fla. Stat. § 501.203(7).

414. 21st Century's conduct occurred in the conduct of "trade and commerce" within the meaning of the FDUTPA, Fla. Stat. § 501.203(8).

415. 21st Century's practices violate the FDUTPA by engaging in unconscionable, deceptive, unfair acts or practices, including, but not limited to:

- a. Failing to maintain adequate and reasonable data security standards to safeguard Florida Subclass members' PI/PHI from unauthorized disclosure,

release, data breaches, and theft, in violation of state and federal laws and its own privacy practices and policies;

- b. Knowingly and fraudulently misrepresenting that it would maintain adequate and reasonable data security standards for Florida Subclass members' PII/PHI and safeguard Florida Subclass members' PII/PHI from unauthorized disclosure, release, data breaches, and theft;
- c. Knowingly omitting, suppressing, and concealing the inadequacy of its data security protections for the Florida Subclass members' PII/PHI;
- d. Failing to disclose the Data Breach to the Florida Subclass members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4); and
- e. Failing to maintain the privacy of medical records and medical information, in violation of Fla. Stat. § 456.057.

416. 21st Century knew or should have known that its computer systems and data security practices and measures failed to meet legal and industry standards, were inadequate to safeguard the Plaintiffs' and Florida Subclass members' PII/PHI and that the risk of a data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate security measures to prevent another breach thereafter.

417. 21st Century's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and members of the Florida Subclass members. Defendants' failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer.

Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and members of the Florida Subclass; and (b) defeat Plaintiffs' and the Florida Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of Defendants' data systems.

418. An objective, reasonable person would have been deceived by 21st Century's representations about the security and protection of data in its databases and networks.

419. Defendants' wrongful practices, which occurred in the course of trade or commerce, were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendants that applied to Plaintiffs and the Florida Subclass and were repeated continuously before and after Defendants obtained confidential PII/PHI concerning Plaintiff and Florida Subclass members, all of whom have been adversely affected by Defendants conduct and the public was and is at risk as a result thereof.

420. 21st Century's acts, omissions, and practices proximately caused Plaintiffs and Florida Subclass members to suffer damages including incurring costs associated with protecting PII/PHI that has been exposed; costs associated with the theft of their identities, such as time and expenses associated with credit monitoring, decrease in credit ratings, financial harm suffered as a result of accounts opened and used without their knowledge or authorization, and time and expense associated with closing accounts opened and used without their knowledge or authorization. Plaintiffs and Florida Subclass members also suffered damages in that they did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) medical goods and services that they

otherwise would not have; and they lost their ability to make informed and reasoned decisions about their medical treatment.

421. As a direct and proximate result of Defendants' unfair and deceptive practices, Plaintiffs and Florida Subclass members also suffered injuries to legally protected interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their PII/PHI, including confidential medical records, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

422. As a direct and proximate cause of these practices, Plaintiff and Florida Subclass members suffered an ascertainable loss.

423. The above unfair and deceptive trade practices and acts by 21st Century were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Florida Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

424. As a direct and proximate result of 21st Century's unlawful, unfair, and fraudulent business practices, Plaintiffs and members of the Florida Subclass have suffered injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining 21st Century from their unlawful and unfair practices.

425. Plaintiffs and the Florida Subclass seek actual damages under Fla. Stat. § 501.211(2) and all fees, costs, and expenses allowed by law, including attorney's fees and

costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, to be proven at trial.

426. Plaintiffs and the Florida Subclass also seek injunctive and declaratory relief, including an order that 21st Century immediately cease and desist its unfair and deceptive acts and practices, under Florida Statutes § 501.211.

427. 21st Century's conduct caused and continues to cause substantial injury to Plaintiffs and Florida Subclass members. 21st Century will continue to maintain Plaintiffs' and Florida Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiffs and Florida Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and Florida Subclass members.

428. Plaintiffs and Florida Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the Florida Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under FDUTPA.

COUNT XVIII
Violations of the Kentucky Consumer Protection Act
Ky. Rev. Stat. §§ 367.170, *et seq.*
(On Behalf of the Kentucky Subclass)

429. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

430. Plaintiff brings this claim on behalf of herself and the Kentucky Subclass.

431. The Kentucky Consumer Protection Act prohibits “[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce.”

432. Pursuant to Kentucky Revised Statute Section 367.110(2), Defendants engaged in “trade” or “commerce” by through the advertisement, sale, and provision of medical services that directly or indirectly affected the people of the Commonwealth of Kentucky.

433. Defendants engaged in deceptive acts or practices by representing to Plaintiff and the Kentucky Subclass that they maintain adequate data security practices and procedures to safeguard Plaintiff’s and Kentucky Subclass’ PII/PHI from unauthorized disclosure, release, data breaches, and theft, and that they would comply with relevant federal and state laws pertaining to the privacy and security of PII/PHI. Plaintiff and the Kentucky Subclass were misled by Defendants’ misrepresentations and reasonably relied upon them to their detriment. Had Plaintiff and the Kentucky Subclass members known about Defendants’ substandard data security practices, they would not have provided their PII/PHI to Defendants or they would have taken steps to protect themselves from harm that could result from Defendants’ substandard data security practices.

434. Defendants engaged in deceptive acts or practices by omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the PII/PHI of Plaintiff and the Kentucky Subclass. At the time that Plaintiff and members of the Kentucky Subclass provided Defendants their PII/PHI for medical services, Defendants failed to disclose to Plaintiff and the Kentucky Subclass that Defendants’ data security systems failed to meet legal and industry standards to protect their PII/PHI. Had Plaintiff and the Subclass known about Defendants’ substandard data security practices, they would not

have provided their PII/PHI to Defendants or they would have taken steps to protect themselves from harm that could result from Defendants' substandard data security practices.

435. 21st Century knew, or should have known, that its data security systems failed to meet legal and industry standards to protect the PII/PHI of Plaintiff and the Kentucky Subclass, were inadequate to safeguard the PII/PHI of Plaintiff and the Kentucky Subclass, and that the risk of a data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate security measures to prevent another breach thereafter. 21st Century's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Kentucky Subclass members.

436. Defendants' failure to disclose such material information rendered their representations of their data security practices as likely to deceive a reasonable consumer. Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Kentucky Subclass; and (b) defeat Plaintiff's and Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of Defendants data systems.

437. An objective, reasonable person would have been deceived by 21st Century's representations about the security and protection of data in its databases and networks.

438. Defendants intended that Plaintiff and the Kentucky Subclass rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with 21st Century's offering of

medical services and incorporating Plaintiff's and Kentucky Subclass members' sensitive information on its computer servers, in violation of the Kentucky Consumer Protection Act.

439. Defendants also engaged in unfair acts and practices, in connection with the sale of medical services by failing to maintain the privacy and security the PII/PHI of Plaintiff and members of the Kentucky Subclass in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including HIPAA (42 U.S.C. § 1302d, *et seq.*).

440. Defendants' wrongful practices, which occurred in the course of trade or commerce, were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendants that applied to Plaintiff and the Kentucky Subclass and were repeated continuously before and after Defendants obtained confidential PII/PHI concerning Plaintiff and Kentucky Subclass members, all of whom have been adversely affected by Defendants conduct and the public was and is at risk as a result thereof.

441. 21st Century's acts, omissions, and practices proximately caused Plaintiff and Kentucky Subclass members to suffer damages including incurring costs associated with protecting PII/PHI that has been exposed; costs associated with the theft of their identities, such as time and expenses associated with credit monitoring, decrease in credit ratings, financial harm suffered as a result of accounts opened and used without their knowledge or authorization, and time and expense associated with closing accounts opened and used without their knowledge or authorization. Plaintiffs and Kentucky Subclass members also

suffered damages in that they did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) medical goods and services that they otherwise would not have; and they lost their ability to make informed and reasoned decisions about their medical treatment.

442. As a direct and proximate result of Defendants' unfair and deceptive practices, Plaintiff and members of the Kentucky Subclass have suffered injuries to legally protected interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their PII/PHI, including confidential medical records, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

443. As a direct and proximate cause of these practices, Plaintiff and Kentucky Subclass members suffered an ascertainable loss.

444. The above unfair and deceptive trade practices and acts by 21st Century were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

445. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices, Plaintiff and members of the Kentucky Subclass have suffered an injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful and unfair practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and

Kentucky Subclass members. 21st Century will continue to maintain Plaintiff's and Kentucky Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and Kentucky Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Kentucky Subclass members.

446. Plaintiff and Kentucky Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Kentucky Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under the Kentucky Consumer Protection Act.

447. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and the Kentucky Consumer Protection Act.

COUNT XIX
Violations of the Massachusetts Consumer Protection Act
Mass. Gen. Laws Ann. Ch. 93A, § 1, *et seq.*
(On Behalf of the Massachusetts Subclass)

448. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

449. Plaintiff is a "person," as meant by Mass. Gen. Laws Ann. ch. 93A, § 1.

450. 21st Century operates in "trade or commerce," as meant by Mass. Gen. Laws Ann. ch. 93A, § 1.

451. 21st Century engaged in deceptive and unfair trade practices in the conduct of trade or commerce in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a). This includes, but is not limited to the following:

- a. 21st Century failed to enact adequate data security measures to protect the Plaintiff's and Massachusetts Subclass members' PII/PHI, including confidential medical records, from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- b. 21st Century failed to take proper action following known security risks and prior cybersecurity incidents including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, to protect the Plaintiff's and Massachusetts Subclass members' PII/PHI, which was a direct and proximate cause of the Data Breach;
- c. 21st Century knowingly and fraudulently misrepresented that it would maintain adequate data security practices and procedures to safeguard Plaintiff's and Massachusetts Subclass members' PII/PHI from undisclosed disclosure, release, data breaches, and theft;
- d. 21st Century omitted, suppressed, and concealed the material fact of the inadequacy of its data security protections from Plaintiff and Massachusetts Subclass members;
- e. 21st Century knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the data security of Plaintiff's and Massachusetts Subclass members' PII/PHI, including but not limited to duties imposed by the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq.*), the Massachusetts Right of Privacy statute,

Mass. Gen. Laws Ann. ch. 214, § 1B, and the Massachusetts data breach statute,

Mass. Gen. Laws Ann. ch. 93H §§ 2(a), 3(a);

f. 21st Century failed to maintain the data security of Plaintiff's and Massachusetts Subclass members' PII/PHI, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach;

g. 21st Century failed to disclose the Data Breach to the Massachusetts Subclass members in a timely and accurate manner, in violation of the duties imposed by Mass. Gen. Laws Ann. ch. 93H, § 3(a); and

h. 21st Century failed to adhere to the data protection requirements of the Massachusetts Data Protection Act, 201 Mass. Code Regs. § 17.00, *et seq.*

452. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and Massachusetts Subclass members have suffered injuries to legally protected interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their PII/PHI, including confidential medical records, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

453. As a direct and proximate cause of these practices, Plaintiff and Massachusetts Subclass members suffered an ascertainable loss.

454. The above unfair and deceptive trade practices and acts by 21st Century were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Massachusetts Subclass members that they could not reasonably avoid; this

substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

455. 21st Century knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Massachusetts Subclass members' PII/PHI, and that the risk of a data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate security measures to prevent another breach thereafter. 21st Century's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Massachusetts Subclass members.

456. A written pre-suit demand under Mass. Gen. Laws Ann. ch. 93A, § 9(3) is unnecessary and unwarranted because 21st Century has long had notice of Plaintiff's allegations, claims and demands, including from the November 13, 2015 notification from the FBI of the Data Breach and 21st Century's own letter notifying Plaintiff and the Massachusetts Subclass members on or about March 2016 of the Data Breach. Further, 21st Century is the party with the most knowledge of the underlying facts giving rise to Plaintiff's allegations, so that any pre-suit notice would not put 21st Century in a better position to evaluate those claims or to aid in negotiation and settlement.

457. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices, Plaintiff and members of the Massachusetts Subclass have suffered an injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful and unfair

practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and Massachusetts Subclass members. 21st Century will continue to maintain Plaintiff's and Massachusetts Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and Massachusetts Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Massachusetts Subclass members.

458. Plaintiff and Massachusetts Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Massachusetts Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under Mass. Gen. Laws Ann. ch. 93A, § 9, including, but not limited to, actual damages, double or treble damages, injunctive and/or other equitable relief.

459. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

COUNT XX
Violations of the Massachusetts Right To Privacy Statute
Mass. Gen. Laws Ann. ch. 214, § 1B.
(On Behalf of the Massachusetts Subclass)

460. Plaintiff incorporate all foregoing factual allegations as if fully set forth herein.

461. Plaintiff is a "person," as meant by Mass. Gen. Laws Ann. ch. 214, § 1B.

462. 21st Century engaged in unreasonable, substantial and serious interference with the privacy of Plaintiff and Massachusetts Subclass members in violation of Mass. Gen. Laws Ann. ch. 214, § 1B. This includes, but is not limited to the following:

a. 21st Century collected and retained the PII/PHI of Plaintiff and Massachusetts Subclass members, not generally known to the public, and thus owed them a duty to exercise reasonable care in implementing administrative, physical and technical safeguards to protect that information, including, but not limited to, maintaining and testing 21st Century's data security systems and taking other reasonable security measures to protect and adequately secure the PII/PHI of Plaintiff and Massachusetts Subclass members from unauthorized access, which it failed to do;

b. 21st Century failed to enact adequate data security measures to protect Plaintiff's and Massachusetts Subclass members' PII/PHI from unauthorized disclosure, release, data breaches and theft, which was a direct and proximate cause of the Data Breach resulting in the public disclosure of Plaintiff's and Massachusetts Subclass members' PII/PHI, including confidential medical records; and

c. 21st Century failed to take proper action following known security risks and prior cybersecurity incidents including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, to employ adequate security measures to protect Plaintiff's and Massachusetts Subclass members' PII/PHI, which was a direct and proximate cause of the Data Breach.

463. The duty 21st Century owed to Plaintiff and Massachusetts Subclass members to protect their PII/PHI is also underscored by Mass. Gen. Laws Ann. ch. 93A, Mass. Gen. Laws Ann. ch. 111, § 70E, Massachusetts data breach statute, Mass. Gen. Laws Ann. ch. 93H, §§ 2(a), 3(a), HIPAA, 42 U.S.C. § 1320d, *et seq.*, and the HITECH Act, 42 U.S.C. § 17901, *et seq.*, which recognize the importance of maintaining the confidentiality of personal

and medical information and were enacted to protect individuals from the unauthorized exposure of their personal and medical information.

464. But for 21st Century's failure to implement and maintain adequate security measures to protect Plaintiff's and Massachusetts Subclass members' PII/PHI, and but for 21st Century's failure to monitor its systems to identify suspicious or unauthorized activity, the PII/PHI of Plaintiff and Massachusetts Subclass members would not have been compromised, they would not have been injured, and they would not be at a heightened risk of identity theft in the future. Thus, there is no legitimate reason for the invasion of Plaintiff's and Massachusetts Subclass members' right to privacy.

465. As a direct and proximate result of 21st Century's violations of Mass. Gen. Laws Ann. ch. 214, § 1B, the PII/PHI of Plaintiff and Massachusetts Subclass members was accessed by unauthorized individuals who continue to use this compromised PII/PHI to commit identity, healthcare and/or medical fraud indefinitely.

466. As a direct and proximate result of 21st Century's violations of Mass. Gen. Laws Ann. ch. 214, § 1B, Plaintiff and Massachusetts Subclass members suffered injuries to legally protected interests, as described above, including, but not limited to, their legally protected interest in the confidentiality and privacy of their PII/PHI, time and expense related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

467. As a direct and proximate result of 21st Century's violations of Mass. Gen. Laws Ann. ch. 214, § 1B, Plaintiff and Massachusetts Subclass members suffered, and will

continue to suffer, injury and/or harm including, but not limited to, anxiety, stress, emotional distress, loss of control over their PII/PHI, and other economic and non-economic losses.

468. As a direct and proximate result of 21st Century's violations of Mass. Gen. Laws Ann. ch. 214, § 1B, Plaintiff and members of the Massachusetts Subclass have suffered an injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful and unfair practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and Massachusetts Subclass members. 21st Century will continue to maintain Plaintiff's and Massachusetts Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and Massachusetts Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Massachusetts Subclass members.

469. Plaintiff and Massachusetts Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Massachusetts Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under Mass. Gen. Laws Ann. ch. 214, § 1B, including, but not limited to, actual damages, double or treble damages, injunctive and/or other equitable relief.

470. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and Mass. Gen. Laws Ann. ch. 214, § 1B..

471. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and Massachusetts Subclass members. 21st Century will continue to maintain

Plaintiff's and Massachusetts Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and Massachusetts Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Massachusetts Subclass members.

472. Plaintiff and Massachusetts Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Massachusetts Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under Mass. Gen. Laws Ann. ch. 214, § 1B.

473. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

COUNT XXI
Violations of the New Jersey Consumer Fraud Act
N.J. Stat. Ann. § 56:8-1, *et seq.*
(On Behalf of the New Jersey Subclass)

474. Plaintiff incorporate all foregoing factual allegations as if fully set forth herein.

475. 21st Century, while operating in New Jersey, engaged in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes, but is not limited to the following:

- a. 21st Century failed to enact adequate data security measures to protect Plaintiff's and New Jersey Subclass members' PII/PHI from unauthorized disclosure,

release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. 21st Century failed to take proper action following known security risks and prior cybersecurity incidents including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, to protect the Plaintiff's and New Jersey Subclass members' PII/PHI, which was a direct and proximate cause of the Data Breach;

c. 21st Century knowingly and fraudulently misrepresented that it would maintain adequate data security practices and procedures to safeguard Plaintiff's and New Jersey Subclass members' PII/PHI from unauthorized disclosure, release, data breaches, and theft;

d. 21st Century omitted, suppressed, and concealed the material fact of the inadequacy of its data security protections from Plaintiff and New Jersey Subclass members;

e. 21st Century knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the data security of Plaintiff's and New Jersey Subclass members' PII/PHI, including but not limited to duties imposed by the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d, *et seq.*); and

f. 21st Century failed to maintain the data security of Plaintiff's and New Jersey Subclass members' PII/PHI, in violation of duties imposed by applicable federal and state laws.

476. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and New Jersey Subclass members suffered injuries to legally protected interests, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII/PHI, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

477. As a direct and proximate cause of these practices, Plaintiff and New Jersey Subclass members suffered an ascertainable loss.

478. The above unfair and deceptive acts and practices and acts by 21st Century were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and New Jersey Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

479. 21st Century knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and New Jersey Subclass members' PII/PHI, and that risk of a data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate security measures to prevent another breach thereafter. 21st Century's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and New Jersey Subclass members.

480. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices, Plaintiff and members of the New Jersey Subclass have suffered an injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful and unfair practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and New Jersey Subclass members. 21st Century will continue to maintain Plaintiff's and New Jersey Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and New Jersey Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and New Jersey Subclass members.

481. Plaintiff and New Jersey Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the New Jersey Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under N.J. Stat. Ann. § 56:8-19, including, but not limited to, actual damages, injunctive and/or other equitable relief and treble damages, and attorneys' fees and costs.

482. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and N.J. Stat. Ann. § 56:8-19.

COUNT XXII
Violations of the Rhode Island Deceptive Trade Practices Act,
R.I. Gen. Laws § 6-13.1, *et seq.*
(On Behalf of the Rhode Island Subclass)

483. Plaintiff incorporate all foregoing factual allegations as if fully set forth herein.

484. Plaintiff brings this claim against 21st Century on behalf of the Rhode Island Subclass.

485. 21st Century's business practices alleged herein constitute unfair and/or deceptive methods, acts, or practices under Rhode Island's Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1.

486. The Rhode Island Subclass members purchased healthcare services from 21st Century in "trade" and "commerce," as meant by R.I. Gen. Laws § 6-13.1-1, for personal, family, and/or household purposes.

487. 21st Century engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Rhode Island Class in violation of R.I. Gen. Laws Ann. § 6-13.1-2, including but not limited to the following:

a. 21st Century misrepresented material facts pertaining to the provision of medical services to the Rhode Island Subclass by representing that they would maintain adequate data security practices and procedures to safeguard Rhode Island Subclass members' PII/PHI from unauthorized disclosure, release, data breaches, and theft in violation of R.I. Gen. Laws Ann. § 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);

b. 21st Century misrepresented material facts pertaining to the provision of medical services to the Rhode Island Subclass by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to

the data security of Rhode Island Class members' PII/PHI in violation of R.I. Gen.

Laws Ann. § 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);

c. 21st Century omitted, suppressed, and concealed the material fact of the inadequacy of the data security protections for Rhode Island Subclass members' PII/PHI in violation of in violation of R.I. Gen. Laws Ann. § 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);

d. 21st Century engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of insurance and health benefits services by failing to maintain the privacy and security of Rhode Island Subclass members' PII/PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq.*), the Rhode Island Confidentiality of Health Care Information Act (R.I. Gen. Laws § 5-37.3-4); and the Rhode Island data breach statute (R.I. Gen. Laws § 11-49.3-2);

e. 21st Century engaged in unlawful, unfair, and deceptive acts and practices with respect to the provision of healthcare services by failing to disclose the Data Breach to Rhode Island Class members in a timely and accurate manner, in violation of R.I. Gen. Laws Ann. § 11-49.2-3(a);

f. 21st Century engaged in the unlawful, unfair, and deceptive acts and practices with respect to the provision of healthcare services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and

protect Rhode Island Subclass members' PII/PHI from further unauthorized disclosure, release, data breaches, and theft.

488. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and Rhode Island Subclass members suffered injuries to legally protected interests, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII/PHI, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII/PHI.

489. As a direct and proximate cause of these practices, Plaintiff and Rhode Island Subclass members suffered an ascertainable loss.

490. The above unlawful, unfair, and deceptive acts and practices by 21st Century were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

491. 21st Century knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Rhode Island Subclass members' PII/PHI, and that risk of a data breach or theft was highly likely, including, but not limited to, its notice of the 2011-2012 Data Breach, as described above, and the lack of employing any adequate security measures to prevent another breach thereafter. 21st Century's actions in engaging in the above-named deceptive acts and practices were

negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and members of the Rhode Island Subclass.

492. As a direct and proximate result of 21st Century's unlawful, unfair, and deceptive acts and practices, the Rhode Island Subclass members suffered an injury in fact, and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful and unfair practices. 21st Century's conduct caused and continues to cause substantial injury to Plaintiff and Rhode Island Subclass members. 21st Century will continue to maintain Plaintiff's and Rhode Island Subclass members' PII/PHI for the indefinite future. Unless injunctive relief is granted, Plaintiff and Rhode Island Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiff and Rhode Island Subclass members.

493. Plaintiff and Rhode Island Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiff and the Rhode Island Subclass have an effective remedy, including enjoining 21st Century from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under R.I. Gen. Laws § 6-13.1-5.2, including, but not limited to, actual damages or \$200 per Subclass member, whichever is greater, injunctive and/or other equitable relief, punitive damages, and attorneys' fees and costs.

494. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

VIII. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and on behalf of the proposed Classes, request that the Court:

- a. Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Interim Co-Lead Counsel, Plaintiffs' Liaison Counsel, Plaintiffs' Local Counsel, and Plaintiffs' Steering Committee as Class Counsel for Plaintiffs to represent the Class;
- b. Find that 21st Century breached its duty to safeguard and protect the PII/PHI of Plaintiffs and Class members that was compromised in the Data Breach;
- c. Award Plaintiffs and Class members appropriate relief, including actual and statutory damages, restitution and disgorgement;
- d. Award equitable, injunctive and declaratory relief as may be appropriate;
- e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;
- f. Award pre-judgment and post-judgment interest as prescribed by law; and
- g. Grant additional legal or equitable relief as this Court may find just and proper.

IX. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: January 17, 2017 Respectfully submitted,

By: /s/ Cari Campen Laufenberg
Cari Campen Laufenberg
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200

Seattle, WA 98101
Telephone: (206) 623-1900
Facsimile: (206) 623-3384
claufenberg@kellerrohrback.com

By: /s/ Daniel S. Robinson
Daniel S. Robinson
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292
drobinson@robinsonfirm.com

Interim Co-Lead Counsel for Plaintiffs

Jodi Westbrook Flowers
MOTLEY RICE LLC
28 Bridgeside Blvd.
Mt. Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
jflowers@motleyrice.com

Robert C. Gilbert
Florida Bar No. 561861
KOPELOWITZ OSTROW
FERGUSON WEISELBERG
GILBERT
2800 Ponce de Leon Blvd., Suite 1100
Coral Gables, FL 33134
Telephone: (305) 529-8858
Facsimile: (954) 525-4300
gilbert@kolawyers.com

***Interim Co-Liaison Counsel for
Plaintiffs***

Kent G. Whittemore
Florida Bar No. 166049
**THE WHITTEMORE LAW GROUP,
P.A.**
100 Second Avenue South, Ste. 304-S

St. Petersburg, FL 33701
Telephone: (727) 821-8752
kwhittemore@wherejusticematters.com

Interim Local Counsel for Plaintiffs

Matthew B. George
**KAPLAN FOX & KILSHEIMER
LLP**
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
mgeorge@kaplanfox.com

Kenneth G. Gilman
Florida Bar No. 340758
GILMAN LAW, LLP
Beachway Professional Center Tower
8951 Bonita Beach Road, S.E. Ste. #525
Bonita Springs, FL 34135
Telephone: (239) 494-6128
kgilman@gilmanlawllp.com

Thomas V. Girardi
GIRARDI | KEESE
1126 Wilshire Boulevard
Los Angeles, CA 90017
Telephone: (213) 977-0211
Facsimile: (213) 481-1554
tgirardi@girardikeese.com

Eric A. Grover
KELLER GROVER LLP
1965 Market Street
San Francisco, CA 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861
eagrover@kellergrover.com

Julie Braman Kane
Florida Bar No. 980277
COLSON HICKS EIDSON, P.A.
255 Alhambra Circle, Penthouse

Coral Gables, Florida 33134
Telephone: (305) 476-7400
Facsimile: (305) 476-7444
julie@colson.com

Steven S. Maher
Florida Bar No. 887846
THE MAHER LAW FIRM, PA
631 W Morse Blvd., Suite 200
Winter Park, FL 32789
Telephone: (407) 839-0866
Facsimile: (407) 425-7958
smaher@maherlawfirm.com

Charles PT Phoenix
Florida Bar No. 0535591
RHODES TUCKER
2407 Periwinkle Way, Suite 6
Sanibel, FL 33957
Telephone: (239) 472-1144
Facsimile: (239) 461-0083
cptp@RhodesTucker.com

Linh G. Vuong
GIRARD GIBBS LLP
601 California St., 14th Floor
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
lgv@girardgibbs.com

Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that on January 17, 2017, I electronically filed the foregoing document with the Clerk of the Court by using the CM/ECF system, which sends notice of electronic filing to all counsel of record.

By: /s/ Cari Campen Laufenberg
Cari Campen Laufenberg

Exhibit C

Data Breach MTD

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION**

IN RE: 21ST CENTURY ONCOLOGY
CUSTOMER DATA SECURITY BREACH
LITIGATION

Case No. 8:16-md-2737-MSS-AEP

MDL No. 2737

**THIS DOCUMENT RELATES TO ALL
CASES**

**DEFENDANTS' MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED
COMPLAINT AND MEMORANDUM IN SUPPORT**

TABLE OF CONTENTS

	Page
MOTION.....	1
MEMORANDUM IN SUPPORT.....	1
I. INTRODUCTION	1
II. STATEMENT OF FACTS	2
III. ARGUMENT	4
A. SEVEN PLAINTIFFS DO NOT HAVE STANDING TO SUE	4
1. The Alleged Increased Risk of Identity Theft or Other Harm Is Insufficient to Establish Standing	4
2. Plaintiffs' Alleged Mitigation Efforts Do Not Support Standing.....	6
3. Plaintiffs' Overpayment Theory Does Not Confer Standing.....	6
4. Plaintiffs' Loss of Value Theory Does Not Confer Standing.....	7
5. The Allegations that Defendants Violated Certain State Statutes Do Not Confer Standing to the Non-misuse Plaintiffs.	7
B. THE REMAINING PLAINTIFFS HAVE FAILED TO STATE A CLAIM.....	8
1. Plaintiffs Have Failed to Plead with Particularity Their Negligent Misrepresentation and Various Deceptive Trade Practices Claims.....	8
2. Plaintiffs' Conclusory Assertions of Fraud by Omission and Purported Active Concealment Do Not Satisfy Rule 9.	11
3. Plaintiffs Have Failed to State a Claim for Breach of Contract.....	12
4. Plaintiffs' Implied Contract Claim Also Fails.	12
5. There Is No Separate Claim for Breach of the Implied Covenant of Good Faith and Fair Dealing.	14
6. Plaintiffs Have Not Alleged Unjust Enrichment.	14

7.	Plaintiffs' Invasion of Privacy Claims Fail Because Defendants Did Not Disclose Plaintiffs' Personal Information.....	15
8.	Plaintiffs' Breach of Fiduciary Duty Claim Also Fails.	16
9.	Plaintiffs Have Failed to Satisfy Required Elements of Several of Their State Statutory Claims.....	17
10.	Plaintiffs' Confidentiality of Medical Information Act Claim Fails.....	19
11.	Plaintiffs Fail to State a Claim Under the Calif. Customer Records Act.....	21
12.	Declaratory and Injunctive Relief (Count XI) Are Not Independent Causes of Action.	22
13.	Plaintiffs' Claims Fail for Lack of Causation.....	22
IV.	CONCLUSION.....	25

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	10, 22
<i>U.S. ex rel. Atkins v. McInteer</i> , 470 F.3d 1350 (11th Cir. 2006)	8
<i>Attias v. CareFirst, Inc.</i> , ---F. Supp. 3d ---, 2016 WL 4250232 (D.D.C. August 10, 2016)	5
<i>Austin-Spearman v. AARP & AARP Servs. Inc.</i> , 119 F. Supp. 3d 1 (D.D.C. 2015).....	10
<i>Badillo v. Playboy Entm't Grp., Inc.</i> , No. 8:04CV591T30TBM, 2006 WL 785707 (M.D. Fla. Mar. 28, 2006).....	17
<i>Bedoya v. United States</i> , No. 2:16-CV-87, 2016 WL 4487872 (S.D. Ga. Aug. 24, 2016).....	22
<i>Blair v. Wachovia Mortg. Corp.</i> , No. 5:11-CV-566-OC-37TBS, 2012 WL 868878 (M.D. Fla. Mar. 14, 2012)	8
<i>Boorstein v. Men's Journal LLC</i> , No. CV 12-771 DSF EX, 2012 WL 2152815 (C.D. Cal. June 14, 2012).....	21
<i>Branca v. Nordstrom, Inc.</i> , No. 14CV2062-MMA JMA, 2015 WL 1841231 (S.D. Cal. Mar. 20, 2015).....	10
<i>Brooks v. Blue Cross and Blue Shield of Fla., Inc.</i> , 116 F.3d 1364 (11th Cir. 1997)	3, 9
<i>Burton v. MAPCO Express, Inc.</i> , 47 F. Supp. 3d 1279 (N.D. Ala. 2014).....	6, 15
<i>Carlsen v. GameStop, Inc.</i> , 112 F. Supp. 3d 855 (D. Minn. 2015), <i>aff'd</i> 833 F.3d 903 (8th Cir. 2016)	7
<i>Case v. Miami Beach Healthcare Grp., Ltd.</i> , 166 F. Supp. 3d 1315 (S.D. Fla. 2016)	5

<i>Cellco P'ship v. Hope,</i> No. CV11-0432 PHX DGC, 2011 WL 3159172 (D. Ariz. July 26, 2011).....	17
<i>Clapper v. Amnesty Int'l USA,</i> -- U.S. --, 133 S. Ct 1138 (2013)	5, 6
<i>In re Cnty. Health Sys.,</i> No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sep. 12, 2016)	5, 7, 22
<i>Corona v. Sony Pictures Entm't, Inc.,</i> No. 14-CV-09600 RGK (Ex.), 2015 WL 3916744 (C.D. Cal. June 15, 2015)	19
<i>Diamond "S" Dev. Corp. v. Mercantile Bank,</i> 989 So. 2d 696 (Fla. Dist. Ct. App. 2008)	15
<i>DiCarlo v. St. Mary Hosp.,</i> 530 F. 3d 255 (D.N.J. 2008)	17
<i>Doe v. Brandeis Univ.,</i> 177 F. Supp. 3d 561 (D. Mass. 2016)	16
<i>Dolmage v. Combined Ins. Co. of Am.,</i> No. 14 C 3809, 2015 WL 292947 (N.D. Ill. Jan. 21, 2015)	16
<i>Eisenhower Medical Center v. Superior Court,</i> 226 Cal. App. 4th 430 (2014)	20, 21
<i>Eveillard v. Nationstar Mortg. LLC,</i> No. 14-CIV-61786, 2015 WL 127893 (S.D. Fla. Jan. 8, 2015).....	21
<i>In re Facebook Privacy Litig.,</i> 791 F. Supp. 2d 705 (N.D. Cal. 2011), <i>aff'd</i> , 572 F. App'x 494 (9th Cir. 2014)	17
<i>Falkenberg v. Alere Home Monitoring, Inc.,</i> No. 13-cv-00341-JST, 2015 WL 800378 (N.D. Cal. Feb. 23, 2015)	20
<i>Flinn v. R.M.D. Corp.,</i> No. 3:11-CV-00386-H, 2012 WL 694037 (W.D. Ky. Mar. 1, 2012)	13
<i>Frezza v. Google, Inc.,</i> No. 12-CV-00237-RMW, 2012 WL 5877587 (N.D. Cal. Nov. 20, 2012).....	13
<i>Green v. eBay, Inc.,</i> No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015).....	6

<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012)	16
<i>Jenkins v. JPMorgan Chase Bank, N.A.</i> , 216 Cal. App. 4th 497 (Cal. Ct. App. 2013)	14
<i>Khan v. Children's Nat'l Health Sys.</i> , 188 F. Supp. 3d 524 (D. Md. 2016)	6, 8
<i>Klein v. Chevron U.S.A., Inc.</i> , 202 Cal. App. 4th 1342 (2012)	15
<i>Kuehn v. Stanley</i> , 91 P.3d 346 (Ariz. Ct. App. 2004)	10
<i>Laccinole v. Assad</i> , No. CV 14-404 S, 2016 WL 868511 (D.R.I. Mar. 7, 2016)	10
<i>Lacy v. BP, PLC</i> , No. 11-CIV-21855, 2015 WL 3952593 (S.D. Fla. June 29, 2015)	8
<i>Law v. Zuckerman</i> , 307 F. Supp. 705 (D. Md. 2004)	17
<i>Lombardo v. Johnson & Johnson Consumer Cos., Inc.</i> , 124 F. Supp. 3d 1283 (S.D. Fla. 2015)	10
<i>Lynch v. Conley</i> , 853 A.2d 1212 (R.I. 2004)	17
<i>In re Managed Care Litig.</i> , 298 F. Supp. 2d 1259 (S.D. Fla. 2003)	17
<i>In re Maple</i> , 434 B.R. 363 (Bankr. E.D. Va. 2010)	12, 18
<i>Merle Wood & Assocs., Inc. v. Trinity Yachts, LLC</i> , 857 F. Supp. 2d 1294 (S.D. Fla. 2012), <i>aff'd</i> , 714 F.3d 1234 (11th Cir. 2013)	13
<i>In re New Motor Vehicles Canadian Exp. Antitrust Litig.</i> , 350 F. Supp. 2d 160 (D. Me. 2004)	18
<i>Nicklaw v. CitiMortgage, Inc.</i> , 839 F.3d 998 (11th Cir. 2016)	4

<i>Peters v. St. Joseph Servs. Corp.,</i> 74 F. Supp. 3d 847 (S.D. Tex. 2015)	6
<i>In re Pharm. Indus. Average Wholesale Price Litig.,</i> 230 F.R.D. 61 (D. Mass. 2005)	18
<i>Purrelli v. State Farm Fire & Cas. Co.,</i> 698 So. 2d 618 (Fla. Dist. Ct. App. 1997)	15
<i>Regents of the Univ. of California v. Superior Court,</i> 220 Cal. App. 4th 549 (2013), as modified on denial of reh'g (Nov. 13, 2013)	19, 20
<i>Remijas v. Neiman Marcus,</i> 794 F.3d 688 (7th Cir. 2015)	5, 6
<i>Resnick v. AvMed, Inc.,</i> 693 F.3d 1317 (11th Cir. 2012)	14, 22
<i>Ruggers, Inc. v. U.S. Rugby Football Union, Ltd.,</i> 843 F. Supp. 2d 139 (D. Mass. 2012)	10
<i>Silver v. Countrywide Home Loans, Inc.,</i> 760 F. Supp. 2d 1330 (S.D. Fla. 2011), aff'd, 483 Fed.Appx. 568 (11th Cir. 2012)	16
<i>Slattery v. Wells Fargo Armored Serv. Corp.,</i> 366 So. 2d 157 (Fla. Dist. Ct. App. 1979)	14
<i>Sleit v. Ricoh Corp.,</i> No. 807-CV-724T-23TBM, 2007 WL 2565967 (M.D. Fla. Aug. 31, 2007)	12
<i>In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,</i> 996 F. Supp. 2d 942 (S.D. Cal. 2014)	21
<i>Spokeo, Inc. v. Robins,</i> 136 S.Ct. 1540 (2016)	4, 8
<i>Stoddard v. Winnebago Indus., Inc.,</i> No. 11CV0370 JAH (BGS), 2012 WL 12846097 (S.D. Cal. Mar. 27, 2012)	18, 19
<i>Storm v. Paytime, Inc.,</i> 90 F. Supp. 3d 359 (M.D. Pa. 2015)	6

<i>Strickland v. United States</i> , 382 F. Supp. 2d 1334 (M.D. Fla. 2005).....	13
<i>In re Supervalu, Inc.</i> , No. 14-MD-2586, 2016 WL 1588105 (D. Minn. Apr. 20, 2016).....	6
<i>Sutter Health v. Superior Court</i> , 227 Cal. App. 4th 1546 (2014), <i>review denied</i> (Oct. 15, 2014).....	19
<i>Torres v. Wendy's Co.</i> , ---F. Supp. 3d ---, 2016 WL 7104257 (M.D. Fla. July 15, 2016).....	5, 6, 7
<i>US Ecology, Inc. v. State of California</i> , 92 Cal. App. 4th 113 (2001)	14
<i>Welborn v. IRS</i> , No. CV 15-1352 (RMC), 2016 WL 6495399 (D.D.C. Nov. 2, 2016)	23
<i>Williams v. Chase Bank USA, N.A.</i> , 390 S.W.3d 824 (Ky. Ct. App. 2012)	18
<i>Willingham v. Global Payments, Inc.</i> , 2013 WL 440702 (N.D. Ga. Feb 5, 2013)	14
<i>World Traveling Fools, LLC v. Diamond Aircraft Indus.</i> , No. 11-61670-CIV, 2015 WL 11143344 (S.D. Fla. Mar. 16, 2015)	11
<i>Zendejas v. Redman</i> , No. 15-81229-CIV-MARRA, 2016 WL 1242349 (S.D. Fla. Mar. 30, 2016)	10
<i>Ziemba v. Cascade Int'l, Inc.</i> , 256 F.3d 1194 (11th Cir. 2001)	11
Statutes	
Cal. Civ. Code § 1782.....	18
Cal. Civ. Code § 1798.81.5.....	21
Cal. Civ. Code § 1798.82.....	21
Cal. Civ. Code § 56, <i>et al.</i> (Confidentiality of Medical Information Act).....	2, 19, 20, 21
Health Insurance Portability and Accountability Act ("HIPAA")..... <i>passim</i>	

Mass. Gen. Laws ch. 93A, § 9(3) 18

Rules

Federal Rule of Civil Procedure 12(b)(1) 1

Federal Rule of Civil Procedure Rule 12(b)(6) 1, 22

Federal Rule of Civil Procedure Rule 9(b) 8, 11

MOTION

Pursuant to Federal Rule of Civil Procedure 12(b)(1) and 12(b)(6), Defendants 21st Century Oncology Investments, LLC and 21st Century Oncology of California (collectively, “21st Century”) move to dismiss Plaintiffs’ Consolidated Class Action Complaint (“Complaint”) (D.E. 100) in its entirety and with prejudice.

MEMORANDUM IN SUPPORT

I. INTRODUCTION

Plaintiffs’ Complaint includes twenty-two separate causes of action arising out of allegations that 21st Century failed to properly secure their network, allowing an unauthorized third party to access Plaintiffs’ personal and medical information (the “Security Incident”). Each Plaintiff’s claims should be dismissed either for lack of Article III standing or for failure to state a claim upon which relief can be granted.

Seven Plaintiffs do not claim to have suffered any form of identity fraud or other misuse of their personal information following the cyberattack, relying only on the possibility of future harm and other novel theories of injury. But these alleged harms are not injuries-in-fact sufficient to satisfy Article III, and therefore, these Plaintiffs lack standing.

All of the Plaintiffs’ claims fail to state a claim upon which relief can be granted. Plaintiffs’ consumer protection and other fraud-based claims are deficient because they have not alleged any specific misrepresentation of fact and have not pled with the required particularity the circumstances surrounding any alleged concealment or omission of fact. Their contract-based claims are inadequate because they cannot point to any express or implied contract that included a promise of data security. Their unjust enrichment claim is

deficient because Plaintiffs do not allege they conferred any benefit on 21st Century other than payments for medical services owed pursuant to an express contract. Their California Confidentiality of Medical Information Act (“CMIA”) claims are lacking because they have not alleged that an unauthorized person actually viewed their confidential medical information. Their invasion of privacy claim fails because they have not alleged an intentional, affirmative disclosure of private information by the Defendants. Their remaining claims fail because they have not alleged facts to plausibly support the conclusion that the Security Incident or any delay in notifying them about it caused their claimed injuries, if any.

II. STATEMENT OF FACTS

In October 2015, 21st Century Oncology, Inc. was the victim of a cyberattack. Compl. ¶ 5. To date, the perpetrators remain unidentified. However, on November 13, 2015, the FBI notified 21st Century Oncology, Inc., that a third party illegally obtained patient information and may have accessed a 21st Century database. *Id.* ¶¶ 5, 96. The FBI subsequently provided 21st Century Oncology, Inc., with a sample of data that an unknown actor posted on the internet. *Id.* ¶ 98. The data provided by the FBI included names, addresses, dates of birth, and Social Security numbers. *Id.* ¶¶ 99-102. The stolen information recovered by the FBI did not include financial information, such as payment card or account numbers. *Id.* While Plaintiffs allege that information recovered by the FBI included “data fields” containing “Protected Health Information,” Plaintiffs do not make—and the documents referenced in the Complaint do not support—any allegation that the data fields containing “Protected Health Information” in the FBI files could be linked to any specific patient, let alone any named Plaintiff. *See id.*

In March 2016, 21st Century Oncology, Inc. sent notification letters to those whose information may have been affected by the cyberattack. *Id.* ¶ 117. The letter informed recipients that the FBI discovered that an unauthorized third party may have accessed a 21st Century database, and that 21st Century immediately hired a leading forensics team to support its investigation into the cyberattack, assess its systems, and bolster security. *Id.*; *see also* Ex. 1.¹ The letter also stated that the intruder may have accessed the database on October 3, 2015, which contained information that may have included the recipient's name, Social Security number, physician's name, diagnosis and treatment information, and insurance information, but that 21st Century had "no evidence that [the recipient's] medical record was accessed" and that 21st Century had "no indication that [the recipient's] information has been misused in any way." Compl. ¶ 121; Ex. 1. In addition, the letter informed recipients that the FBI asked that 21st Century delay notification or public announcement of the incident up to that point so as not to interfere with its investigation. *Id.* ¶ 117, Ex. 1. The letter also indicated that, "out of an abundance of caution," 21st Century was offering a free one-year membership of Experian's ProtectMyID Alert. *Id.* ¶ 206; Ex. 1.

¹This Court can consider Exhibit 1 (form letter used for March 4, 2016 notification letter) because Plaintiffs have incorporated it by reference. *Brooks v. Blue Cross and Blue Shield of Fla., Inc.*, 116 F.3d 1364, 1368 (11th Cir. 1997) (documents submitted by a defendant with a motion to dismiss, rather than by the plaintiff with the complaint, may be considered by the court if "the plaintiff refers to [those] documents in the complaint and those documents are central to the plaintiff's claim").

III. ARGUMENT

A. SEVEN PLAINTIFFS DO NOT HAVE STANDING TO SUE.

Seven Plaintiffs (the “non-misuse plaintiffs”)² have not alleged that any of their personal information has been misused following the Security Incident or that they have suffered any actual economic losses. Compl. ¶¶ 21, 30, 35, 45, 49, 83 (alleging that they “anticipate[] spending considerable time and money to contain the impact of the Data Breach”). Instead, these non-misuse plaintiffs rely on several alternative theories of injury: 1) the risk of future identity theft; 2) payment of money or time spent attempting to mitigate future harms; 3) 21st Century’s failure to prevent the cyberattack means they somehow “overpaid” for their healthcare services; 4) the value of their PII/PHI has somehow diminished as a consequence of the cyberattack; and 5) 21st Century’s failure to prevent the cyberattack violated one or more state statutes. None of these theories support Article III standing. To justify standing to sue for claims arising from risk of harm, Article III requires a concrete risk of certainly impending harm—not harm that is conjectural or hypothetical.

See Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1548 (2016); *Nicklaw v. CitiMortgage, Inc.*, 839 F.3d 998, 1003 (11th Cir. 2016).

1. The Alleged Increased Risk of Identity Theft or Other Harm Is Insufficient to Establish Standing.

The non-misuse plaintiffs have no present injury but claim to have standing based on their belief that they face an increased risk of identity theft—seeking to sue 21st Century to recover damages for something that has not yet happened, and something that may never happen. Compl. ¶¶ 4, 119. But mere “[a]llegations of *possible* future injury . . . are not

²Robert Russell, Roxanne Haatvedt, Veneta Delucchi, Matthew Benzion, Kathleen LaBarge, Sharon MacDermid, and James Corbel.

sufficient.” *Clapper v. Amnesty Int’l USA*, -- U.S. --, 133 S. Ct 1138, 1147 (2013) (emphasis in original) (quotation omitted). For a future injury to give rise to Article III standing, it must be “certainly impending.” *Id.* at 1151.

The Eleventh Circuit Court of Appeals has not addressed what facts must be pled to support the conclusion that the victim of a data breach faces “certainly impending” harm sufficient to satisfy the *Clapper* standard. However, the majority view among the district courts within this Circuit has been that plaintiffs who have not suffered any identity fraud or other misuse of their personal information cannot rely on the mere possibility that identity theft or misuse will occur in the future to establish Article III standing. *See, e.g., Case v. Miami Beach Healthcare Grp., Ltd.*, 166 F. Supp. 3d 1315, 1319 (S.D. Fla. 2016) (no standing because “Case did not allege that any of her sensitive information was misused, or that she suffered any negative consequences from the data breach”); *In re Cmyt. Health Sys. (“CHS”)*, No. 15-CV-222-KOB, 2016 WL 4732630, at *10 (N.D. Ala. Sep. 12, 2016) (plaintiffs who had not alleged some form of identity theft or other misuse did not have standing). The case most cited for the contrary view, *Remijas v. Neimen Marcus*, 794 F.3d 688 (7th Cir. 2015), has been criticized outside the Seventh Circuit, and it is distinguishable because it involved allegations that mass payment card fraud was already occurring (9,200 cards known to be fraudulently used), so that even those plaintiffs who had not yet suffered fraudulent charges could be seen as facing a certainly impending risk of the same. *See CHS*, 2016 WL 4732630, at *10 (distinguishing *Remijas*).³

³Various other federal court decisions are in agreement. *See, e.g., Torres v. Wendy’s Co.*, ---F. Supp. 3d ---, 2016 WL 7104257, at *4-*5 (M.D. Fla. July 15, 2016) (distinguishing *Remijas* and finding no standing despite the fact that plaintiff alleged two fraudulent charges to a debit card that were reimbursed by his credit union because such allegations could not establish out-of-pocket monetary damages); *Attias v. CareFirst, Inc.*, ---F.

2. Plaintiffs' Alleged Mitigation Efforts Do Not Support Standing.

The non-misuse plaintiffs next claim they have standing because they spent time or money attempting to mitigate the risk of future identity theft or other harm. But “plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Wendy’s*, 2016 WL 7104257, at *5 (quoting *Clapper*, 133 S.Ct. at 1151). In fact, “[t]he majority of courts in data breach cases have held that the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent.” *Id.* (citing *In re Supervalu, Inc.*, 2016 WL 1588105 at *7); *Khan v. Children’s Nat’l Health Sys.*, 188 F. Supp. 3d 524, 531 (D. Md. 2016) (collecting cases). Time and effort spent mitigating the risks of harm *in the absence of any misuse* do not constitute an injury in fact. *See Wendy’s*, 2016 WL 7104257, at *5.

3. Plaintiffs’ Overpayment Theory Does Not Confer Standing.

The non-misuse plaintiffs also claim that they have suffered an alleged overpayment “for healthcare services purchased, in that a portion of that amount paid . . . was for the costs for 21st Century to take reasonable and adequate security measures to protect [their] PII/PHI.” Compl. ¶ 200(h). Courts across the country have held that this “overpayment” theory fails to establish injury in fact, particularly where, as here, “Plaintiffs [do] not allege

Supp. 3d ---, 2016 WL 4250232, at *3-*4 (D.D.C. August 10, 2016) (distinguishing *Remijas* and finding that Plaintiffs’ “theory of injury is still too speculative to satisfy *Clapper*,” even though some Plaintiffs alleged tax-refund fraud, because the alleged injury was not “fairly traceable to the challenged action”); *In re Supervalu, Inc.*, No. 14-MD-2586, 2016 WL 1588105, at *2 (D. Minn. Apr. 20, 2016) (stating that the “Court is unpersuaded by the rationale” used in *Remijas* and its progeny “to change its conclusion that plaintiffs failed to meet the burden of establishing an injury in fact for purposes of Article III standing”); *Green v. eBay, Inc.*, No. 14-1688, 2015 WL 2066531, at *3-6 (E.D. La. May 4, 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 367 (M.D. Pa. 2015); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 854-55 (S.D. Tex. 2015); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1284-85 (N.D. Ala. 2014); *In re Science Appl. Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 Supp. 3d 14, 25-28 (D.D.C. 2014).

that they paid anything *specific* for the protection; that patients who did not pay for services received a *different level of protection* from those who did pay; that Plaintiffs *paid a premium* for data protection or otherwise bargained for the protection; or that Plaintiffs received *any information about data protection other than a HIPAA Notice.*” CHS, 2016 WL 4732630, at *7 (emphasis added); *see also Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 861 (D. Minn. 2015), *aff’d* 833 F.3d 903 (8th Cir. 2016) (“Courts have generally found ‘overpayment’ theories insufficient to establish injury, even in situations involving highly sensitive [personal information].” (collecting cases)).

4. Plaintiffs’ Loss of Value Theory Does Not Confer Standing.

The non-misuse plaintiffs also argue that as a result of the cyberattack, they have incurred “damages to and diminution in value of their PII/PHI.” Compl. ¶ 200(f). This theory has also been rejected by multiple courts, including courts in this Circuit, as a basis to establish Article III standing when, as in this case, the plaintiffs cannot plausibly allege that they intended to sell their personal or medical information. *See, e.g., Wendy’s*, 2016 WL 7104257, at *5 (rejecting loss of value theory despite allegations that “there is an established national and international market for this data,” because “Plaintiff does not explain how this information became less valuable after the Data Breach”); *see also CHS*, 2016 WL 4732630, at *9 (“Even if [Plaintiffs] did intend to sell their own data—something no one alleges—it is unclear whether or how the data has been devalued by the breach.”).

5. The Allegations that Defendants Violated Certain State Statutes Do Not Confer Standing to the Non-misuse Plaintiffs.

Finally, the non-misuse plaintiffs allege violations of certain of their state statutes. Compl. at Counts XII, XIV, XVI-XIX, XXI-XXII. However, the Supreme Court made clear

that “Article III requires a concrete injury even in the context of a statutory violation.” *Spokeo*, 136 S. Ct. at 1543. And there is “no authority for the proposition that a state legislature [], through a state statute or cause of action, can manufacture Article III standing for a litigant who has not suffered a concrete injury.” *See Khan*, 188 F. Supp. 3d at 534.

B. THE REMAINING PLAINTIFFS HAVE FAILED TO STATE A CLAIM.

1. Plaintiffs Have Failed to Plead with Particularity Their Negligent Misrepresentation and Various Deceptive Trade Practices Claims.

Plaintiffs base their negligent misrepresentation claim (Count IV) and various deceptive trade practices claims (Counts XII, XIV, XVI-XIX, XXI-XXII) on the allegation that 21st Century “misrepresented material facts . . . by representing they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs’ and Class members’ PII/PHI,” and “by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiffs’ and Class members’ PII/PHI.” Compl. ¶¶ 268-69. These allegations fail to satisfy Rule 9(b)’s heightened pleading standard. *See, e.g., Lacy v. BP, PLC*, No. 11-CIV-21855, 2015 WL 3952593, at *3 (S.D. Fla. June 29, 2015) (“A plaintiff alleging state law fraud claims must satisfy the heightened pleading standard of Rule 9(b).”); *Blair v. Wachovia Mortg. Corp.*, No. 5:11-CV-566-OC-37TBS, 2012 WL 868878, at *3 (M.D. Fla. Mar. 14, 2012) (applying Rule 9(b) to FDUTPA claim “where the gravamen of the claim sounds in fraud”).

Plaintiffs are required to state “facts as to time, place, and substance of the defendant’s alleged fraud” and “details of the defendant[’s] allegedly fraudulent acts, when they occurred, and who engaged in them.” *U.S. ex rel. Atkins v. McInteer*, 470 F.3d 1350,

1357 (11th Cir. 2006). Nowhere in the Complaint's 494 paragraphs do Plaintiffs identify any specific statement that either of the Defendants made regarding data security or their efforts to comply with any data security law, let alone the time and place of any such statement.

The only document referenced in the Complaint that could conceivably be the foundation for Plaintiffs' assertions that Defendants made misrepresentations to them is 21st Century's HIPAA privacy notice. Compl. ¶¶ 8, 132.⁴ But the plain language of the HIPAA privacy notice does not contain any representations (let alone *misrepresentations*) about the quality of 21st Century's data security measures or their efforts to comply with any federal or state law and cannot be the basis for a fraud claim. Plaintiffs cite the following two sentences from the notice in their Complaint:

[W]e are required by law to maintain the privacy of your protected health information, to provide you with notice of our legal duties and privacy practices with respect to that protected health information, and to notify any affected individuals following a breach of any unsecured protected health information. We will abide by the terms of the notice currently in effect.

Id. (quoting Ex. 2).⁵ The quoted excerpt from the notice is merely a statement that HIPAA regulations require 21st Century to maintain the privacy of patient health information and to provide a notice that describes *its own use and disclosure of patient information for certain permitted purposes*. See 45 C.F.R. § 164.520(b); Ex. 2, at 1. Any argument that the privacy notice includes a false or deceptive statement about data security ignores what the document

⁴Plaintiffs also characterize as "false and/or misleading" the March 4, 2016 letter notifying them about the Security Incident. However, 21st Century sent this letter *after* discovery of the Security Incident, so statements contained within it cannot form the basis of any fraud claim permitting Plaintiffs to recover damages that allegedly arose from the Security Incident itself. In any event, the Complaint contains no allegations that any Plaintiff suffered any particular injury or loss as a result of having relied on statements in the March 4, 2016 letter.

⁵Exhibit 2 (21st Century Oncology, LLC Notice of Privacy Practices, Mar. 26, 2013, available at <https://www.21co.com/company/hipaa-notice-of-privacy-practices> (last visited January 30, 2017)), has been incorporated by reference into the Complaint, thus, this Court may consider it. *Brooks*, 116 F.3d at 1368.

actually says and cannot plausibly form a basis for a fraudulent misrepresentation claim.

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (allegations that state “no more than conclusions” are “not entitled to the assumption of truth”); *Austin-Spearman v. AARP & AARP Servs. Inc.*, 119 F. Supp. 3d 1, 10 (D.D.C. 2015) (“such a promise [alleged by Plaintiffs] is not even close to what the actual Privacy Policy says, no matter how many times Plaintiff makes this assertion.”).

Even if the HIPAA privacy notice had contained any statements about data security (it does not), Plaintiffs allege no facts to support the conclusion that *any* of them read, let alone relied on, those statements before seeking healthcare from 21st Century.⁶ For their negligent misrepresentation claims, Plaintiffs must establish actual, justifiable reliance to state a claim. *See, e.g., Zendejas v. Redman*, No. 15-81229-CIV-MARRA, 2016 WL 1242349, at *6 (S.D. Fla. Mar. 30, 2016) (applying Florida law); *Kuehn v. Stanley*, 91 P.3d 346, 349 (Ariz. Ct. App. 2004). Also, several of the state consumer protection statutes on which Plaintiffs base their claims require a plaintiff to plead actual reliance when a violation is based on a false or fraudulent statement. *See, e.g., Kuehn*, 91 P.3d at 351 (ACFA); *Branca v. Nordstrom, Inc.*, No. 14CV2062-MMA JMA, 2015 WL 1841231, at *3 (S.D. Cal. Mar. 20, 2015) (UCL and CLRA); *Ruggers, Inc. v. U.S. Rugby Football Union, Ltd.*, 843 F. Supp. 2d 139, 147 (D. Mass. 2012) (MCPA).⁷

⁶In fact, Plaintiff Robert Russell does not allege that he ever received medical services from 21st Century, so it is impossible for him to allege any reliance whatsoever.

⁷Even those laws that do not require actual reliance still require a plaintiff to plead facts that support the conclusion that the alleged misrepresentation would mislead a reasonable consumer. *See, e.g., Lombardo v. Johnson & Johnson Consumer Cos., Inc.*, 124 F. Supp. 3d 1283, 1290 (S.D. Fla. 2015) (“to prove the causation element of a FDUTPA claim,” a plaintiff must “prove that an objectively reasonable person would have been deceived.”) (citation omitted); *Laccinole v. Assad*, No. CV 14-404 S, 2016 WL 868511, at *8 (D.R.I. Mar. 7, 2016) (“[f]or conduct to be deceptive it must, among other things, be likely to mislead a reasonable

2. Plaintiffs' Conclusory Assertions of Fraud by Omission and Purported Active Concealment Do Not Satisfy Rule 9.

In addition to alleging affirmative misrepresentations, Plaintiffs also allege that Defendants engaged in deceptive or fraudulent acts or practices “by omitting, suppressing, and concealing the material fact of the inadequacy of their data security protections” and that Defendants “failed to disclose . . . that [their] data security systems failed to meet legal and industry standards.” Compl. ¶¶ 344 (ACFA, Count XII).⁸ These claims also fail to satisfy Rule 9 because Plaintiffs offer no clear articulation of what precisely should have been disclosed to them and when it should have been disclosed. *See Ziembra v. Cascade Int'l, Inc.*, 256 F.3d 1194, 1202 (11th Cir. 2001) (Rule 9(b) requires a Plaintiff to state “precisely what . . . omissions were made”).

Furthermore, Plaintiffs’ concealment claims require that a defendant intentionally misled or gave materially incorrect information to the Plaintiff to send that party down the wrong path. *See, e.g., World Traveling Fools, LLC v. Diamond Aircraft Indus.*, No. 11-61670-CIV, 2015 WL 11143344, at *5 (S.D. Fla. Mar. 16, 2015) (“Fraudulent concealment involves deceptive acts or contrivances intended to hide information, mislead, avoid suspicion, or prevent further inquiry into a material matter.”) (citation omitted). Plaintiffs plead no facts that could meet this requirement. Instead, they make the conclusory statement that Defendants “suppressed and concealed,” without explaining how and when.

consumer...”). Here, no consumer would reasonably conclude that the statements in the privacy notice, all of which pertain only to permitted use of data under HIPAA, promised a particular quality of data security.

⁸*See also* Compl. ¶¶ 379 (UCL, Count XIV), 415(c) (FDUTPA, Count XVII), 434 (KCPA, Count XVIII), 451(d) (MCPA, Count XIX), 475(d) (NJCPA, Count XXI), and 487(c) (RIDTPA, Count XXII) (all alleging that Defendants either omitted, suppressed, or concealed the “inadequacy” of their data security).

3. Plaintiffs Have Failed to State a Claim for Breach of Contract.

Plaintiffs have not pled facts sufficient to support the conclusion that they entered into an express contract with Defendants containing a promise of data security. The sole written document Plaintiffs reference in the Complaint in support of their assertion that this contract exists is 21st Century's HIPAA privacy notice. Compl. ¶¶ 279 & n.81, 280. But as discussed above, the privacy notice does not discuss data security nor can it be a contract for data security. *See In re Maple*, 434 B.R. 363, 371 (Bankr. E.D. Va. 2010) (rejecting “the conclusory allegation that there exists some unexplained legally enforceable contractual obligation between Plaintiffs and Defendant in the form of a HIPAA privacy policy”).

In addition, the privacy notice cannot be a contract because it is not supported by any consideration. HIPAA regulations *require* healthcare providers to provide the notice. 45 C.F.R. § 164.520(a)(1). Because Defendants had a preexisting legal duty to provide the notice, and because the requirements in the notice are themselves created by federal law, the notice is not a legally enforceable agreement. *See, e.g., In re Maple*, 434 B.R. at 371 (holding that HIPAA privacy policy did not constitute a “legally enforceable agreement between the parties upon which Plaintiffs purport to rely”); *Sleit v. Ricoh Corp.*, No. 807-CV-724T-23TBM, 2007 WL 2565967, at *1 (M.D. Fla. Aug. 31, 2007) (a policy statement is a unilateral promise that does not create a contract).

4. Plaintiffs' Implied Contract Claim Also Fails.

Plaintiffs base their implied contract claim on the allegation that they “were required to provide their PII/PHI to obtain healthcare from affiliated providers of 21st Century, and/or 21st Century” (Compl. ¶ 292) and that they entered into implied contracts “for the provision

of adequate data security, separate and apart from any express contracts concerning health care, whereby 21st Century was obligated to take reasonable steps to secure and safeguard that information”⁹ (*Id.* ¶ 293).

This claim fails because Plaintiffs do not allege facts sufficient to plausibly show a mutual intent to contract and an offer and acceptance, which are required elements even for an implied contract. *Strickland v. United States*, 382 F. Supp. 2d 1334, 1343 (M.D. Fla. 2005). The only statements made by Defendants that Plaintiffs identify to support the existence of the implied contract come from a privacy notice, which does not contain any specific representations or promises regarding data security. Moreover, no Plaintiff alleges ever reading the privacy notice, or any other document discussing privacy or data security, when he or she sought healthcare. The lack of an allegation that any Plaintiff read the privacy notice is fatal to the use of that document to create an implied contract. *See, e.g., Frezza v. Google, Inc.*, No. 12-CV-00237-RMW, 2012 WL 5877587, at *4 (N.D. Cal. Nov. 20, 2012) (rejecting implied contract claim where plaintiffs did not “sufficiently plead that Google agreed to and then breached a specific obligation” to comply with data security standards). Without alleging the basic elements of an implied contract, that Plaintiffs understood certain conduct or a document they *read* as an offer to provide any data security measures, or that they accepted the purported offer on its terms, Plaintiffs’ claim necessarily

⁹ Plaintiffs do not specify whether they intend to bring an action for breach of contract implied in law or implied in fact; however, a claim for breach of contract implied in law is treated the same as a claim for unjust enrichment because both are “an obligation created by the law.” *See Merle Wood & Assocs., Inc. v. Trinity Yachts, LLC*, 857 F. Supp. 2d 1294, 1306 (S.D. Fla. 2012), *aff’d*, 714 F.3d 1234 (11th Cir. 2013); *Flinn v. R.M.D. Corp.*, No. 3:11-CV-00386-H, 2012 WL 694037, at *3 (W.D. Ky. Mar. 1, 2012) (same). Here, Plaintiffs have a claim for unjust enrichment already (Count IX), which is addressed below.

fails.¹⁰ See *Willingham v. Global Payments, Inc.*, 2013 WL 440702, at *20 (N.D. Ga. Feb 5, 2013).

Further, because HIPAA and other state data security laws required 21st Century to guard individuals' PII/PHI, the preexisting duty rule bars a contract claim for alleged breach of these duties. *US Ecology, Inc. v. State of California*, 92 Cal. App. 4th 113, 129 (2001) ("A promise to perform a preexisting legal duty is not supported by consideration."); *Slattery v. Wells Fargo Armored Serv. Corp.*, 366 So. 2d 157, 159 (Fla. Dist. Ct. App. 1979) (same).

5. There Is No Separate Claim for Breach of the Implied Covenant of Good Faith and Fair Dealing.

The duty of good faith must "relate to the performance of an express term of the contract." *Avmed*, 693 F.3d at 1329; *see also Jenkins v. JPMorgan Chase Bank, N.A.*, 216 Cal. App. 4th 497, 525 (Cal. Ct. App. 2013). Because Plaintiffs fail to allege the existence of contractual terms (express or implied), their claim for breach of the implied covenant of good faith and fair dealing also fails. Moreover, even if Plaintiffs did allege applicable contractual terms, the claim would still fail because Plaintiffs allege that the claim was prompted by 21st Century's alleged negligence, not a conscious and deliberate act.

6. Plaintiffs Have Not Alleged Unjust Enrichment.

Plaintiffs allege 21st Century has been unjustly enriched by retaining Plaintiffs' payments for medical care while providing allegedly inadequate data security. But no

¹⁰Although the Court in *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324-28 (11th Cir. 2012), found that the plaintiffs there sufficiently pled a claim for breach of implied contract, *Avmed* is distinguishable for multiple reasons. First, the plaintiffs had attached a written "service contract" to their complaint, which required AvMed "to ensure the 'confidentiality of information about members' medical health condition being maintained by the Plan.'" *Id.* at 1329. No such guarantees are alleged here, nor are they present in the privacy notice. Second, the analysis in *Avmed* for breach of implied contract was limited only to the "causation element," which, unlike here, the plaintiffs satisfied by pleading detailed facts sufficient to show that they took precautions to protect their confidential information and they had never before been victims of identity theft. *Id.* at 1325-26.

Plaintiff actually alleges that he or she paid any money out of pocket for medical services from 21st Century, and some do not allege they even received treatment from 21st Century. *See, e.g.*, Compl. ¶ 7 (“21st Century is not a name known to all Class members”), ¶ 18 (Plaintiff Robert Russell alleges 21st Century possessed his PII/PHI but never alleges he received medical services). Absent plausible facts to establish Plaintiffs conferred a benefit on 21st Century, they have not even pled facts to satisfy the first element of this claim.

Moreover, it is black letter law that “a plaintiff cannot pursue a quasi-contract claim for unjust enrichment if an express contract exists concerning the same subject matter.”

Diamond “S” Dev. Corp. v. Mercantile Bank, 989 So. 2d 696, 697 (Fla. Dist. Ct. App. 2008); *Klein v. Chevron U.S.A., Inc.*, 202 Cal. App. 4th 1342, 1388 (2012) (“While generally parties are permitted to plead in the alternative, the allegation of binding contracts nullifies the unjust enrichment claim.”). Here, to the extent any of the Plaintiffs paid money to 21st Century, they did so pursuant to an express contract with 21st Century for *medical services*, and they therefore cannot rely on an unjust enrichment theory in an attempt to recover any portion of those payments they allege were attributable to data security.

7. Plaintiffs’ Invasion of Privacy Claims Fail Because Defendants Did Not Disclose Plaintiffs’ Personal Information.

Plaintiffs claim that 21st Century’s allegedly negligent failure to prevent the cyberattack constitutes an invasion of privacy. Compl. at Count X and ¶¶ 5, 10, 323, 325, 335, 374-75, 451a-b. However, a common law invasion of privacy claim requires that the tortfeasor *intentionally disclose* private facts. *Purrelly v. State Farm Fire & Cas. Co.*, 698 So. 2d 618, 620 (Fla. Dist. Ct. App. 1997) (“[I]nvasion of privacy can only be actionable if done intentionally.”); *see also Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1288 (N.D.

Ala. 2014) (“Even if the defendants were negligent, as alleged, in safeguarding Mr. Burton’s account information, such negligence does not morph into an intentional act of divulging his confidential information.”). Because Plaintiffs make no allegations that 21st Century affirmatively and intentionally *disclosed* their information, these claims all fail.¹¹

8. Plaintiffs’ Breach of Fiduciary Duty Claim Also Fails.

Plaintiffs improperly base their breach of fiduciary duty claim on the conclusory allegation that “[a]s guardians of [Plaintiffs’] PII/PHI,” 21st Century “owed a fiduciary duty to Plaintiff and the Class.” Compl. ¶ 317. The mere receipt of confidential information is insufficient to create a fiduciary relationship. *See Silver v. Countrywide Home Loans, Inc.*, 760 F. Supp. 2d 1330, 1338 (S.D. Fla. 2011), *aff’d*, 483 Fed.Appx. 568 (11th Cir. 2012) (holding “the mere communication of confidential information between the borrower and the bank is not enough to establish a fiduciary obligation”); *see also Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *6 (N.D. Ill. Jan. 21, 2015) (allegations that plaintiff and class members placed trust in defendant regarding handling, maintenance, and disposition of confidential personal information were insufficient to establish a fiduciary duty).

¹¹The same is true under California law (Compl. ¶ 331) and for a claim for a violation of the Massachusetts Right to Privacy Statute (Count XX), both of which require allegations that a defendant actually affirmatively disclosed a plaintiff’s confidential information. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (stating that “[e]ven negligent conduct that leads to theft of highly personal information . . . does not ‘approach [the] standard’ of actionable conduct under the California Constitution and thus does not constitute a violation of Plaintiffs’ right to privacy”); *Doe v. Brandeis Univ.*, 177 F. Supp. 3d 561, 616-17 (D. Mass. 2016) (requiring facts “indicating that [defendant] either ‘actively participated in or substantially assisted’ disclosure of personal information to a third party”).

9. Plaintiffs Have Failed to Satisfy Required Elements of Several of Their State Statutory Claims.

First, to be considered a “consumer” for purposes of the California UCL, Arizona ACFA, and Florida FDUTPA, a plaintiff must pay money to the defendant. *See, e.g., In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011), *aff’d*, 572 F. App’x 494 (9th Cir. 2014) (applying California law and noting that only “a plaintiff who is a *consumer* of certain services (i.e., who ‘paid fees’ for those services) may state a claim” (emphasis in original)); *Cellco P’ship v. Hope*, No. CV11-0432 PHX DGC, 2011 WL 3159172, at *4 (D. Ariz. July 26, 2011) (ACFA); *Badillo v. Playboy Entm’t Grp., Inc.*, No. 8:04CV591T30TBM, 2006 WL 785707, at *6 (M.D. Fla. Mar. 28, 2006) (FDUTPA). Here, none of the Plaintiffs has specifically alleged that he or she personally paid 21st Century for any medical services. This omission is especially significant in light of the fact that health insurance commonly covers the cost of medical services.

The New Jersey NJCFA excludes “representation[s] involving the rendering of services by a learned professional,” which includes all activities related to the services of healthcare providers. *See DiCarlo v. St. Mary Hosp.*, 530 F. 3d 255, 268 (D.N.J. 2008) (noting courts apply the exclusion generally to hospital practices); *see also In re Managed Care Litig.*, 298 F. Supp. 2d 1259, 1304 (S.D. Fla. 2003) (“provision of medical services . . . does not constitute the ‘sale’ of ‘merchandise’”). Plaintiffs here concede that “Defendants provide a full spectrum of cancer services” (Compl. ¶ 93), and all but one allege that they “received medical services” from Defendants, making their claims exempt from the NJCFA.

Under the Rhode Island RIDTPA, if the “general activities complained of are subject to monitoring or regulation by a state or federal government agency,” then they are exempt

from the Act. *Lynch v. Conley*, 853 A.2d 1212, 1214 (R.I. 2004). Here, Plaintiffs concede that Defendants are subject to HIPAA and HITECH laws (Compl. ¶¶ 138-150), which exist to “protect the security and privacy of individually identifiable health information.” *Law v. Zuckerman*, 307 F. Supp. 705, 711 (D. Md. 2004). “HIPAA directly assigns the authority to enforce HIPAA to the Secretary of Health and Human Services,” making compliance of HIPAA monitored, supervised and regulated by government agencies. *In re Maple*, 434 B.R. at 370. Thus, the activities complained about here are squarely within the exemption.

Plaintiffs’ Kentucky KCPA claim fails because the Act cannot be used to bring a class action as a matter of law. *See In re Pharm. Indus. Average Wholesale Price Litig.*, 230 F.R.D. 61, 84 (D. Mass. 2005) (“[U]nder the laws of . . . Kentucky . . . there is no right to bring a class action to enforce the consumer protection statute[.]”). And even if Plaintiffs could bring a claim under Kentucky’s statute as a class action (they cannot), the plaintiff “must be a purchaser with privity of contract in order to have standing to bring an action under the Act.” *Williams v. Chase Bank USA, N.A.*, 390 S.W.3d 824, 829 (Ky. Ct. App. 2012). As explained above, Plaintiffs have not adequately alleged a contractual relationship with Defendants.

The Massachusetts MCPA and California CLRA both require thirty-days written notice with a demand for relief before filing an action. *See* Cal. Civ. Code § 1782 and Mass. Gen. Laws ch. 93A, § 9(3). The statutory notice requirements are strictly applied in both states. *See, e.g., In re New Motor Vehicles Canadian Exp. Antitrust Litig.*, 350 F. Supp. 2d 160, 188-89 (D. Me. 2004) (applying Massachusetts law) (“[T]he initial complaints filed across the country and the Amended Complaint filed in this Court . . . cannot ‘effectively act

as the required notice.”’); *see also Stoddard v. Winnebago Indus., Inc.*, No. 11CV0370 JAH (BGS), 2012 WL 12846097, at *7-*8 (S.D. Cal. Mar. 27, 2012) (statement in complaint that “Plaintiffs intend service of this Complaint to constitute notice” insufficient). Because Plaintiffs do not allege that they provided notice before filing their Complaint, their CLRA claim is also subject to dismissal with prejudice. *Stoddard*, 2012 WL 12846097, at *7-*8.

10. Plaintiffs’ Confidentiality of Medical Information Act Claim Fails.

Under the California CMIA, a plaintiff must allege that an unauthorized third party actually viewed his or her medical information. *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546 (2014), *review denied* (Oct. 15, 2014) and *Regents of the Univ. of California v. Superior Court*, 220 Cal. App. 4th 549 (2013), *as modified on denial of reh’g* (Nov. 13, 2013).¹² In their Complaint, Plaintiffs never affirmatively plead that an unauthorized party actually viewed their confidential medical information, nor do they plead any other facts that, if true, would support the reasonable inference that a viewing occurred, without resorting to impermissible “layers of speculation.” *Regents*, 220 Cal. App. 4th at 570 n.15. At best, Plaintiffs’ allegations support the conclusion that a database containing their medical information was accessed and that this information may have been stolen or acquired by unauthorized third persons, which were the exact same allegations held to be insufficient by the Court of Appeals in both *Regents* and *Sutter*.

¹² In *Sutter Health* and *Regents*, the California Court of Appeals expressly rejected the argument that the CMIA “authorize[s] a private cause of action for damages based solely on the negligent maintenance or storage of medical information even if the patient’s confidential records were never viewed.” *Regents*, 220 Cal. App. 4th at 553-54; *accord, Sutter Health*, 227 Cal. App. 4th at 1555. To state any of the above claims under the CMIA, a plaintiff must allege a “breach of confidentiality,” which does not “take[] place until an unauthorized person views the medical information.” *Sutter Health*, 227 Cal. App. 4th at 1557; *see also Regents*, 220 Cal. App. 4th at 561 (same).

Plaintiffs have also not alleged facts that have permitted other CMIA claims to survive motions to dismiss. For example, Plaintiffs have not alleged that there has been any sort of publication of their confidential medical information following the Security Incident. *Cf. Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *1, 8 (C.D. Cal. June 15, 2015) (medical conditions of specific individuals was not only “posted on the internet,” but was also “used to threaten the [plaintiffs] and their families”). Although Plaintiffs allege that various data regarding PII, including names, addresses and birth dates, were acquired online by the FBI (Compl. ¶¶ 99-104), they never allege that any confidential *medical* information specific to any patient or Plaintiff was included in that data. Instead, Plaintiffs only refer to “Protected Health Information,” which is not the same as the CMIA’s definition of “confidential medical information.” Compl. ¶¶ 99, 101-102; *See Eisenhower Medical Center v. Superior Court*, 226 Cal. App. 4th 430, 435 (2014) (holding that “medical information” as defined by the CMIA does not mean “just any patient-related information held by a health care provider, but must . . . include a patient’s *medical history, mental or physical condition, or treatment*” (emphasis added)).

Finally, no allegations support the inference that criminals might have accessed certain Plaintiffs’ medical information because those Plaintiffs also suffered identity theft. For instance, the plaintiffs in *Falkenberg v. Alere Home Monitoring, Inc.*, No. 13-cv-00341-JST, 2015 WL 800378, at *1, *3 (N.D. Cal. Feb. 23, 2015), avoided dismissal because they alleged that not only was their confidential medical information stolen, but also that they contemporaneously suffered actual identity theft, that they “had never before suffered identity theft,” and that they “always took extra precautions to ensure their confidential

information was not disclosed to unknown third parties.” None of the Plaintiffs in this case has made similar allegations.¹³

11. Plaintiffs Fail to State a Claim Under the Calif. Customer Records Act.

Plaintiffs allege a violation of California Civil Code section 1798.81.5 (Count XV), but the provisions of section 1798.81.5 do not apply to “[a] provider of health care, health care service plan, or contractor regulated by the [CMIA].” *Id.* at (e)(1). Plaintiffs concede that 21st Century is a “‘provider of health care’ pursuant to [] the CMIA.” Compl. ¶ 361. Thus, 21st Century cannot be liable under section 1798.81.5. Plaintiffs also allege that 21st Century violated Civil Code section 1798.82, but this section does not provide a statutory remedy and thus, to recover actual compensatory damages, Plaintiffs must plead and prove those damages. *Boorstein v. Men’s Journal LLC*, No. CV 12-771 DSF EX, 2012 WL 2152815, at *4 (C.D. Cal. June 14, 2012) (alleging a violation of section 1798.82 not enough; a plaintiff must allege an actual injury resulting from the violation). The only harm Plaintiffs allege is that the alleged delay in notification put them at a “heightened risk of identity theft” and “tax fraud.” Compl. ¶ 118. These allegations fail to assert any cognizable harm from the theft itself, let alone any harm from any alleged lack of sufficient notice or delay in providing notice of the theft. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*,

¹³ Mr. Corbel’s additional factual allegation that he “began receiving suspicious telephone calls” does not save the Complaint from dismissal. Compl. ¶ 25. Nearly identical allegations were rejected as insufficient to state a claim in *Regents* because, even accepting them as true, they would require additional layers of speculation to equate to an allegation that someone actually viewed the plaintiff’s confidential *medical* information. 220 Cal. App. 4th at 570 n.15. Similarly here, Mr. Corbel’s alleged harm indicates only that some unidentified scammers have his telephone number, which is not confidential information, let alone confidential *medical* information, and could have been obtained by other means. *Eisenhower Med. Ctr.*, 226 Cal. App. 4th at 435.

996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (plaintiffs failed to allege how the *delay*, as opposed to the intrusion itself, caused their alleged damages).

12. Declaratory and Injunctive Relief (Count XI) Are Not Independent Causes of Action.

Plaintiffs' claim for "Declaratory and Injunctive Relief" fails as it is not an independent cause of action. *See Eveillard v. Nationstar Mortg. LLC*, No. 14-CIV-61786, 2015 WL 127893, at *9 (S.D. Fla. Jan. 8, 2015) ("Declaratory relief ... cannot stand on its own."); *see also Bedoya v. United States*, No. 2:16-CV-87, 2016 WL 4487872, at *3 (S.D. Ga. Aug. 24, 2016), *recommendation adopted*, No. 2:16-CV-87, 2016 WL 5402757 (S.D. Ga. Sept. 26, 2016) ("no such thing as a suit for a traditional injunction in the abstract.").

13. Plaintiffs' Claims Fail for Lack of Causation.

All of Plaintiffs' remaining claims, including their negligence and gross negligence claims, also fail because Plaintiffs have not adequately alleged the element of causation. Generally, to prove that a data breach caused identity theft, "Plaintiffs cannot rest merely upon time and sequence that the alleged fact of misuse occurred after the data breach." *CHS*, 2016 WL 4732630, at *26; *Iqbal*, 556 U.S. at 678 (under Rule 12(b)(6), "facts that are 'merely consistent with' a defendant's liability" are insufficient). The Eleventh Circuit has held that to avoid dismissal for failure to plead causation, a plaintiff must plead facts sufficient to rule out other causes. *See Avmed*, 693 F.3d at 1327 (recognizing that the plaintiffs alleged that they took special precautions to protect their PII/PHI and had not been victims of other data security breaches in the past, and noting that "[h]ad Plaintiffs alleged fewer facts, we doubt whether the Complaint could have survived a motion to dismiss").

Here, Plaintiffs vaguely plead attempts of misuse that rely *only* on time and sequence to connect them to the cyberattack. In fact, the acts of misuse Plaintiffs claim involve information that was not even alleged to have been compromised by the cyberattack or was information that an unauthorized user could have easily obtained elsewhere. For example, Plaintiffs Schmitt, Meulenberg, and Griffith all allege unauthorized access to bank accounts or payment cards, but they do not allege the cyberattack included information identifying bank accounts or bank credentials. Compl. ¶¶ 37, 59, 72. Likewise, Mr. Schmitt alleges that he received a phishing email but does not allege that the cyberattack involved his email address. Compl. ¶ 37. Mr. Brehio alleges that his eBay account was “used fraudulently” but similarly fails to allege or explain how the cyberattack at an oncology center directly led to a third party using his eBay login credentials. Compl. ¶ 86.

And, even though Plaintiffs allege Social Security numbers were generally involved in the cyberattack, most Plaintiffs cannot allege any connection from the alleged stolen Social Security numbers to their alleged misuse. For example, Mr. Schmitt alleges that someone attempted to open an Amazon credit card in his name, but he does not allege that his Social Security number was used to do so. Compl. ¶ 37. Mr. Meulenberg alleges that an unauthorized party attempted to apply for two credit cards using his PII, but he does not allege that his Social Security number was specifically used. Compl. ¶ 59. Ms. Griffith alleges that attempts were made to “access her credit card” and to make purchases using her name on Amazon, but she does not allege that her Social Security number was used in either case. Compl. ¶ 72. Ms. Cabrera alleges that she “received an alert from LifeLock notifying her that her PII had been ‘given away, traded or sold,’” but she fails to allege whether any of

the PII included her Social Security number or any of the information allegedly involved in the cyberattack. Compl. ¶ 77. Similarly, Ms. Schwartz alleges that on August 1, 2016 “an unknown third party attempted to apply for a Chase credit card using his PII,” without identifying the PII used. Compl. ¶ 53. None of these allegations include facts sufficient to support proximate causation. *See, e.g., Welborn v. IRS*, No. CV 15-1352 (RMC), 2016 WL 6495399, at *9 (D.D.C. Nov. 2, 2016) (analyzing causation in the standing context and holding that allegations that fraud happened after data breach are insufficient where “[i]t is not clear that the type of data obtained from the theft . . . was necessarily used in the [fraudulent] removal of funds.” (citing *SAIC*, 45 F.Supp.3d at 31)).

Further, even in the two instances where Plaintiffs allege that Social Security numbers were involved in the alleged misuse, there still are no allegations linking the misuse to the cyberattack. Mr. Wilbur alleges that his health insurance “had been cancelled” and that his insurance agent informed him that his Social Security number “had been compromised,” but he fails to allege whether these two incidents are linked and when this information was compromised, instead only alleging when he learned it had been compromised. Compl. ¶ 62. Indeed, it is plausible that this information was compromised prior to the cyberattack. Mr. Brehio alleges that two cell phones were opened in his name in July 2016, that his eBay account was “used fraudulently” around the same time, and someone used his name, Social Security number, and date of birth to attempt to open a credit card in his name in August 2016. Compl. ¶ 86. However, because these activities occurred within a month of each other—and nearly ten months after the cyberattack—it is more plausible that they are all inextricably intertwined with a separate and unrelated incident.

None of these allegations are sufficient to suggest a nexus beyond allegations of time and sequence because there are myriad of other explanations for how a third party could have obtained any of this information, including a phone book, a public records search, the breach of another consumer account (bank, insurer, utility, etc.), a stolen wallet, an unsecure wireless network connection, stolen mail, a garbage sifter, or numerous other possibilities. Out of several million people whose information may have been compromised in the cyberattack, Plaintiffs identify only seven individuals who allege to have suffered attempted identity theft after the cyberattack. This amounts to a .000003 percent rate of alleged identity theft—far below the national average. *See SAIC*, 45 F. Supp. 3d at 32 (“[i]n a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud.”).

No facts in the Complaint, if true, would rule out any of these other possibilities, let alone all of them, leaving nothing but speculation to bridge the gap between allegations of attempted identity fraud and the Security Incident.

IV. CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court dismiss Plaintiffs’ Complaint for want of standing and failure to state a claim.

Respectfully submitted on February 21, 2017.

BAKER & HOSTETLER LLP

By: /s/ Paul G. Karlsgodt
Casic D. Collignon
Paul G. Karlsgodt
Zachariah J. DeMeola
1801 California Street, Suite 4400
Denver, CO 80202-2662
Telephone: (303) 861-0600
Facsimile: (303) 861-7805
ccollignon@bakerlaw.com
pkarlsgodt@bakerlaw.com
zdemeola@bakerlaw.com

Jerry R. Linscott
Florida Bar Number 148009
BAKER & HOSTETLER LLP
200 South Orange Ave., Suite 2300
Orlando, FL 32801-3432
Telephone: (407) 649-4000
Facsimile: (407) 841-0168
jlinscott@bakerlaw.com

*Counsel for Defendants 21st Century
Oncology Investments, LLC and 21st
Century Oncology of California*

CERTIFICATE OF SERVICE

I certify that a true and correct copy of the foregoing **MOTION TO DISMISS AND
MEMORANDUM IN SUPPORT** was served via the Court's ECF system on all counsel of record on this 21st day of February, 2016.

/s/ Paul G. Karlsgodt